3499014894S1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

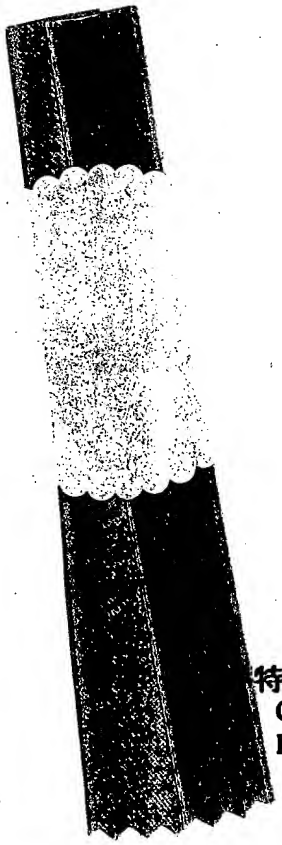
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１０月２２日

出願番号
Application Number: 平成１１年特許願第３０１２１６号

出願人
Applicant (s): 株式会社日立製作所



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ４月１４日

特許庁長官
Commissioner,
Patent Office 近藤隆

出証番号 出証特２０００－３０２６５２７

【書類名】　特許願

【整理番号】　HL12666000

【提出日】　平成11年10月22日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L　9/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　宮崎　邦彦

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　佐々木　良一

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　宝木　和夫

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　洲崎　誠一

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　森津　俊之

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報システム事業部内

【氏名】　酒井　瑞洋

【発明者】
【住所又は居所】　東京都練馬区中村２－１４－１７
【氏名】　岩村　充
【発明者】
【住所又は居所】　神奈川県横浜市青葉区柿の木台１３－４５
【氏名】　松本　勉
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100087170
【弁理士】
【氏名又は名称】　富田　和子
【電話番号】　045(316)3711
【手数料の表示】
【予納台帳番号】　012014
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】明細書

【発明の名称】デジタル署名方法および装置

【特許請求の範囲】

【請求項１】

メッセージに対するデジタル署名を検証するデジタル署名方法であって、

デジタル署名生成者側の装置において、

メッセージあるいはそのハッシュ値に、デジタル署名生成者が所有する秘密鍵を作用させ、当該メッセージに対するデジタル署名を生成する署名生成ステップと、

生成したデジタル署名とメッセージを含むデジタル署名付きメッセージを配布するとともに、当該デジタル署名付きメッセージのログデータをログリストに登録する登録ステップと、を有し、

デジタル署名検証者側の装置において、

配布されたデジタル署名付きメッセージを、検証対象デジタル署名付きメッセージとして受け付ける検証対象受付ステップと、

前記検証対象デジタル署名付きメッセージを配布したデジタル署名者のログリストを取得する履歴取得ステップと、

前記検証対象デジタル署名付きメッセージのログデータが、前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証対象デジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであることを認証する第１の検証ステップと、を有すること

を特徴とするデジタル署名方法。

【請求項２】

請求項１記載のデジタル署名方法であって、

前記登録ステップは、デジタル署名付きメッセージのログデータを、前記デジタル署名者側の装置とは別に設けられた履歴管理センタが管理するログリストに登録すること

を特徴とするデジタル署名方法。

出証特２０００－３０２６５２７

【請求項３】

請求項１または２記載のデジタル署名方法であって、

前記デジタル署名検証者側の装置において、

前記第１の検証ステップに先立ち、前記検証対象デジタル署名付きメッセージに含まれるメッセージおよびデジタル署名と、前記秘密鍵と対の公開鍵とを用いて、前記検証対象デジタル署名付きメッセージに含まれるデジタル署名が当該検証対象デジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項４】

請求項１または２記載のデジタル署名方法であって、

前記署名生成ステップは、メッセージあるいはそのハッシュ値と、前記ログリストに登録されている最新のログデータに含まれるデータ（前データ）とに、前記秘密鍵を作用させて、当該メッセージに対するデジタル署名を生成し、

前記登録ステップは、生成したデジタル署名と前データとメッセージを含むデジタル署名付きメッセージを配布するとともに、当該デジタル署名付きメッセージのログデータをログリストに登録すること

を特徴とするデジタル署名方法。

【請求項５】

請求項４記載のデジタル署名方法であって、

デジタル署名検証者側の装置において、

前記第１の検証ステップに先立ち、前記検証対象デジタル署名付きメッセージに含まれるデジタル署名、前データおよびメッセージと、前記秘密鍵と対の公開鍵とを用いて、前記検証対象デジタル署名付きメッセージに含まれるデジタル署名が当該検証対象デジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項６】

請求項４または５記載のデジタル署名方法であって、

前記デジタル署名検証者側の装置において、

前記第１の検証ステップにより、前記検証対象デジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであると認証された場合に、前記検証対象デジタル署名付きメッセージに含まれる前データが、前記ログリストにて前記検証対象デジタル署名付きメッセージのログデータより１つ前に登録されているログデータに含まれているか否かを調べ、含まれている場合は、前記ログリストが改竄されていないことを認証する第３の検証ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項７】

請求項４または５記載のデジタル署名方法であって、

前記登録ステップは、デジタル署名付きメッセージのログデータを、配布先を付してログリストに登録し、

前記デジタル署名検証者側の装置において、

前記第１の検証ステップにより、検証対象デジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであると認証された場合に、前記ログリストにて前記検証対象デジタル署名付きメッセージのログデータより１つ前に登録されているログデータに付された配布先から、デジタル署名付きメッセージを取得し、これが前記１つ前に登録されているログデータに含まれているか否かを調べ、含まれている場合は、前記ログリストが改竄されていないことを認証する第４の検証ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項８】

請求項２記載のデジタル署名方法であって、

前記署名生成ステップは、メッセージあるいはそのハッシュ値と、前記ログリストに登録されている最新のログデータに含まれるデータ（前データ）とに、前記秘密鍵を作用させて、当該メッセージに対するデジタル署名を生成し、

前記登録ステップは、生成したデジタル署名と前データとメッセージを含むデジタル署名付きメッセージを配布するとともに、当該デジタル署名付きメッセー

ジのログデータを前記履歴管理センタが管理するログリストに登録し、かつ、

前記履歴管理センタにおいて、

前記登録ステップによるログデータのログリストへの登録に先立ち、前記検証対象デジタル署名付きメッセージに含まれる前データが、前記ログリストに登録されている最新のログデータに含まれている場合にのみ、当該ログデータの前記ログリストへの登録を許可する登録許可ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項９】

メッセージに対するデジタル署名を生成するデジタル署名装置であって、

メッセージあるいはそのハッシュ値に秘密鍵を作用させ、当該メッセージに対するデジタル署名を生成する署名生成手段と、

生成したデジタル署名とメッセージを含むデジタル署名付きメッセージのログデータを、記憶手段に格納されたログリストに登録する登録手段と、を有すること

を特徴とするデジタル署名装置。

【請求項１０】

請求項９記載のデジタル署名装置であって、

前記署名生成手段は、メッセージあるいはそのハッシュ値と、前記ログリストに登録されている最新のログデータに含まれるデータ（前データ）とに、前記秘密鍵を作用させ、当該メッセージに対するデジタル署名を生成し、

前記登録手段は、生成したデジタル署名とメッセージと前データを含むデジタル署名付きメッセージのログデータを、前記ログリストに登録すること

を特徴とするデジタル署名装置。

【請求項１１】

請求項９または１０記載のデジタル署名装置であって、

当該デジタル署名装置は、電子計算機に接続可能に構成された、前記記憶手段を有する計算機能付き記憶媒体であること

を特徴とするデジタル署名装置。

【請求項１２】

請求項１１記載のデジタル署名装置であって、

前記登録手段は、前記記憶手段に格納されたログリストに、新たに生成したデジタル署名付きメッセージのログデータを登録する場合、当該ログリストに登録されるログデータの数が所定数を超える場合は、当該ログリストに登録されているログデータのうち最も古いログデータを、前記電子計算機に出力して、前記電子計算機に用意されたログリストに登録するとともに、当該最も古いログデータを前記記憶手段から削除してから、新たに生成したデジタル署名付きメッセージのログデータを登録すること

を特徴とするデジタル署名装置。

【請求項１３】

請求項９記載のデジタル署名装置で生成されたデジタル署名を検証するデジタル署名検証装置であって、

検証すべきデジタル署名付きメッセージと前記デジタル署名装置の記憶手段に格納されているログリストを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証すべきデジタル署名付きメッセージが、前記デジタル署名装置が関与して生成されたものであることを認証する第１の検証手段と、

前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名およびメッセージと、前記デジタル署名装置が所持する秘密鍵と対の公開鍵とを用いて、前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名が当該検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証手段と、を有すること

を特徴とするデジタル署名検証装置。

【請求項１４】

請求項１０記載のデジタル署名装置で生成されたデジタル署名を検証するデジタル署名検証装置であって、

検証すべきデジタル署名付きメッセージと前記デジタル署名装置の記憶手段に

格納されているログリストを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証すべきデジタル署名付きメッセージが、前記デジタル署名装置が関与して生成されたものであることを認証する第１の検証手段と、

前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名、前データおよびメッセージと、前記デジタル署名装置が所持する秘密鍵と対の公開鍵とを用いて、前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名が当該検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証手段と、

前記検証すべきデジタル署名付きメッセージに含まれる前データが、前記ログリストにて前記検証すべきデジタル署名付きメッセージのログデータより１つ前に登録されているログデータに含まれているか否かを調べ、含まれている場合は、前記ログリストが改竄されていないことを認証する第３の検証手段と、を有すること

を特徴とするデジタル署名検証装置。

【請求項１５】

請求項９記載のデジタル署名装置で生成されたデジタル署名を検証するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読取られ実行されることで、

検証すべきデジタル署名付きメッセージと前記デジタル署名装置の記憶手段に格納されているログリストを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証対象デジタル署名付きメッセージが、前記デジタル署名装置が関与して生成されたものであることを認証する第１の検証手段とを、前記電子計算機上に構築すること

を特徴とする記憶媒体。

【請求項１６】

メッセージに対するデジタル署名を検証するデジタル署名方法であって、

デジタル署名生成者側の装置において、

メッセージあるいはそのハッシュ値に、デジタル署名生成者が所有する秘密鍵を作用させてデジタル署名を生成する署名生成ステップと、

前記デジタル署名を信頼できる第３者であるタイムスタンプ発行局に送信し、その応答としてタイムスタンプを得るタイムスタンプ取得ステップと、

取得したタイムスタンプを前記メッセージに付し、デジタル署名付きメッセージとして配布する配布ステップと、を有し、

タイムスタンプ発行局側の装置において、

デジタル署名生成者から送られてきたデジタル署名と当該デジタル署名の受信時刻を含むデータに、タイムスタンプ発行局が所有する秘密鍵を作用させ、タイムスタンプを生成するタイムスタンプ生成ステップと、

前記タイムスタンプを前記デジタル署名生成者に送信する送信ステップと、を有し、

デジタル署名検証者側の装置において、

配布されたデジタル署名付きメッセージを、検証対象デジタル署名付きメッセージとして受け付ける検証対象受付ステップと、

前記検証対象デジタル署名付きメッセージに含まれるタイムスタンプに、タイムスタンプ発行局が所有する秘密鍵と対の公開鍵を作用させ、デジタル署名と時刻データを得る署名取得ステップと、

取得した時刻データが示す日時が、前記デジタル署名生成者より予め通知された期限を過ぎているか否かを調べ、過ぎていない場合は、取得したデジタル署名を有効と認証する第１の検証ステップと、を有すること

を特徴とするデジタル署名方法。

【請求項１７】

請求項１６記載のデジタル署名方法であって、

前記デジタル署名検証者側の装置において、

前記第１の検証ステップにより、デジタル署名が有効であると認証された場合に、当該デジタル署名と、前記検証対象デジタル署名付きメッセージに含まれるメッセージと、前記デジタル署名生成者の秘密鍵と対の公開鍵とを用いて、前記

デジタル署名が前記デジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証ステップを、さらに有することを特徴とするデジタル署名方法。

【請求項１８】

メッセージに対するデジタル署名を生成するデジタル署名システムであって、

デジタル署名装置とタイムスタンプ発行装置とを備え、

前記デジタル署名装置は、

メッセージあるいはそのハッシュ値に、自装置が所持する秘密鍵を作用させ、デジタル署名を生成する署名生成手段と、

前記デジタル署名を前記タイムスタンプ発行装置に送信し、その応答としてタイムスタンプを得るタイムスタンプ取得手段と、

取得したタイムスタンプを前記メッセージに付し、デジタル署名付きメッセージを作成する署名付きメッセージ作成手段と、を有し、

前記タイムスタンプ発行装置は、

前記デジタル署名生成装置から送られてきたデジタル署名と当該デジタル署名の受信時刻を含むデータに、自装置が所持する秘密鍵を作用させ、タイムスタンプを生成するタイムスタンプ生成手段と、

前記タイムスタンプを前記デジタル署名生成装置に送信する送信手段と、を有すること

を特徴とするデジタル署名システム。

【請求項１９】

請求項１８記載のデジタル署名システムで生成されデジタル署名を検証するデジタル署名検証装置であって、

検証すべきデジタル署名付きメッセージを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージに含まれるタイムスタンプに、前記タイムスタンプ発行装置が所持する秘密鍵と対の公開鍵を作用させ、デジタル署名と時刻データを得る署名取得手段と、

前記署名取得手段で取得した時刻データが示す日時が、前記デジタル署名装置の使用者より予め通知された期限を過ぎているか否かを調べ、過ぎていない場合

は、前記デジタル署名を有効と認証する第１の検証手段と、

前記デジタル署名と、前記検証すべきデジタル署名付きメッセージに含まれるメッセージと、前記デジタル署名生成装置が所持する秘密鍵と対の公開鍵とを用いて、前記デジタル署名が前記検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証手段と、を有すること

を特徴とするデジタル署名検証装置。

【請求項２０】

請求項１８記載のデジタル署名システムで生成されデジタル署名を検証するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読取られ実行されることで、

検証すべきデジタル署名付きメッセージを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージに含まれるタイムスタンプに、前記タイムスタンプ発行装置が所持する秘密鍵と対の公開鍵を作用させ、デジタル署名と時刻データを得る署名取得手段と、

前記署名取得手段で取得した時刻データが示す日時が、前記デジタル署名装置の使用者より予め通知された期限を過ぎているか否かを調べ、過ぎていない場合は、前記デジタル署名を有効と認証する第１の検証手段と、

前記署名取得手段で取得したデジタル署名と、前記検証すべきデジタル署名付きメッセージに含まれるメッセージと、前記デジタル署名生成装置が所持する秘密鍵と対の公開鍵とを用いて、前記デジタル署名が前記検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第２の検証手段とを、前記電子計算機上に構築すること

を特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル署名技術に関する。

【０００２】

【従来の技術】

電子的な文書などのデジタル化されたメッセージに、従来の印鑑に相当する機能を付与する技術であるデジタル署名が、電子商取引などにおけるネットワークの高度利用を可能にする技術として、注目されつつある。

【０００３】

デジタル署名技術に関する文献としては、たとえば以下のものがある。

【０００４】

文献１： Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography" CRC Press, Inc. 1997

文献２： Bruce Schneier, "Applied Cryptography Second Edition", Jogn Wiley & Sons, Inc. 1996

文献３： International Application Number PCT/US91/05386

文献４： "Standerd Specifications for Public Key Cryptography (Draft Version 11)" IEEE P1363, IEEE, July 1999

上記の各文献に記載のデジタル署名技術では、デジタル署名生成者は、署名対象となるメッセージMあるいはそのメッセージダイジェストであるハッシュ値に、自身が秘密裏に保持する秘密鍵を作用させることで、メッセージMに対するデジタル署名Aを生成する。そして、メッセージMにデジタル署名Aを付して公開する。一方、デジタル署名検証者は、メッセージMに付されたデジタル署名Aを前記秘密鍵と対の公開鍵を作用させることで得た結果と、メッセージMあるいはそのハッシュ値とを比較する。両者が一致しない場合は、デジタル署名Aが生成された後にメッセージMに何らかの改竄が加えられた可能性がある。このため、両者が一致する場合にのみ、デジタル署名Aがメッセージに対してなされたものであることを認証する。

【０００５】

なお、上記の文献２のP75、"CHAPTER4 Intermediate Protocols, 4.1 TIMESTANPING SERVICES"や文献３には、デジタル署名生成者が、自身が生成したメッセージに何らかの改竄を加えて新たにデジタル署名を生成し、これらを元のメッセ

ージおよびデジタル署名と置き換えるような不正な行為を防止する技術が開示されている。該技術では、デジタル署名生成者は、署名対象となるメッセージM_nあるいはそのハッシュ値と１つ前に生成したデジタル署名A_{n-1}と時刻データを、自身が秘密裏に保持する秘密鍵を作用させることで、メッセージM_nに対するデジタル署名A_nを生成する。このようにすると、デジタル署名A_nの次に生成されるデジタル署名A_{n+1}には、１つ前に生成したデジタル署名A_nが反映される。このため、デジタル署名生成者が自身が生成したメッセージM_nに何らかの改竄を加えて新たにデジタル署名A_nを生成し、これらを元のメッセージM_nおよびデジタル署名A_nと置き換えるような不正な行為を行うと、デジタル署名A_{n+1}との間で整合がとれなくなる。

【０００６】

【発明が解決しようとする課題】

ところで、上記のデジタル署名技術では、デジタル署名生成者が自身の秘密鍵を秘密裏に保持していることが前提となっている。すなわち、前記秘密鍵と対の公開鍵を用いて検証することができるデジタル署名を生成できるものは、前記秘密鍵を保持するデジタル署名生成者のみであることを前提としている。デジタル署名生成者の秘密鍵管理の不手際など何らかの理由により、第３者がデジタル署名生成者の秘密鍵を不正に入手し、デジタル署名生成者になりすましてデジタル署名を行った場合、上記のデジタル署名技術では、これを検知することができない。

【０００７】

なお、 International Application Number PCT/US93/1117には、メッセージと当該メッセージに対するデジタル署名に、デジタル署名生成者が保持する新たな秘密鍵を作用させることで、メッセージに対するデジタル署名を新たに生成する技術が開示されている。しかしながら、該技術は、近年の電子計算機の演算能力の飛躍的な向上や公開鍵から秘密鍵を求めるアルゴリズムの改良などにより、第３者がデジタル署名生成者の秘密鍵を不正に入手できる可能性が高まってきた場合に、以前に行ったデジタル署名のセキュリティを確保するための技術であり、秘密鍵を不正に入手した第３者がデジタル署名生成者になりすまして行ったデ

ジタル署名を検知することはできない。

【０００８】

本発明は上記事情に鑑みてなされたものであり、本発明の目的は、デジタル署名生成者自身がしたデジタル署名と第３者がデジタル署名生成者になりすまして行ったデジタル署名とを識別可能なデジタル署名技術を提供することにある。

【０００９】

【課題を解決するための手段】

上記目的を達成するために、本発明の第１の態様は、デジタル署名生成者側において、生成したデジタル署名とメッセージを含むデジタル署名付きメッセージの配布に先立ち、当該デジタル署名付きメッセージのログデータをログリストに登録する。ここで、ログデータとは、デジタル署名付きメッセージそのものであってもよいし、あるいは、デジタル署名付きメッセージに含まれるメッセージを当該メッセージのハッシュ値に置き換えたデジタル署名付きメッセージであってもよい。

【００１０】

このようにすることで、デジタル署名検証者は、デジタル署名生成者からログリストを入手し、検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べることで、当該検証すべきデジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであるか否かを検証することが可能となる。

【００１１】

また、本発明の第２の態様は、デジタル署名生成者側において、自らが生成したメッセージに対するデジタル署名を、信頼できる第３者であるタイムスタンプ発行局に送信し、タイムスタンプ発行局が秘密裏に保持する秘密鍵を用いて当該デジタル署名と時刻データを暗号化し、タイムスタンプを生成してもらう。そして、このタイムスタンプを前記メッセージに付して配布する。

【００１２】

このようにすることで、デジタル署名検証者は、タイムスタンプ発行局の秘密鍵と対の公開鍵を用いて、メッセージに付されたタイムスタンプから時刻データ

とデジタル署名を取得し、この時刻データが示す日時が、デジタル署名生成者より予め通知された日時を過ぎているか否かを調べることで、デジタル署名が、デジタル署名生成者が有効と認めるものか否かを検証することが可能となる。

【００１３】

【発明の実施の形態】

以下に本発明の実施の形態について説明する。

【００１４】

まず、本発明の第１実施形態について説明する。

【００１５】

図１は本発明の第１実施形態が適用されたシステムの概略図である。

【００１６】

図示するように、本システムは、デジタル署名付きメッセージを作成するデジタル署名者側装置1_1～1_n（以下、単にデジタル署名者側装置1とする）と、デジタル署名者側装置1が作成したデジタル署名付きメッセージを保持する購入者側装置3_1～3_n（以下、単に購入者側装置3とする）と、デジタル署名者側装置1が作成したデジタル署名付きメッセージの検証を行うデジタル署名検証者側装置5と、デジタル署名者側装置1が作成したメッセージのリストを公開し、購入者側装置3に代わってデジタル署名付きメッセージをデジタル署名者側装置1より入手する仲介者側装置7とを含んで構成される。

【００１７】

なお、本発明の実施の形態において、メッセージとは、電子的な文書などのデジタルデータの他、イメージデータや音声データなどのデジタル化されたマルチメディアデータや、有価証券と同じ価値を持つデジタルデータなども含むものとする。また、本発明の実施の形態の説明にて用いられれる文言「購入」とは、有償無償を問わず、デジタル署名者が作成したデジタル署名付きメッセージを何らかの方法により入手する行為を指すものとする。

【００１８】

図２は、デジタル署名者側装置1の概略構成図である。

【００１９】

図示するように、デジタル署名者側装置1は、CPU11と、CPU11のワークエリアとして機能するRAM12と、ハードディスク装置などの外部記憶装置13と、CD-ROMやFDなどの可搬性を有する記憶媒体15からデータを読取る読取り装置14と、キーボードやマウスなどの入力装置16と、ディスプレイなどの表示装置17と、ネットワークを介して他の装置と通信を行うための通信装置18と、ICカード接続装置19と、上述した各構成要素間のデータ送受を司るインターフェース20を備えた、一般的な構成を有する電子計算機21に、計算機能付き記憶媒体であるICカード22を接続することで構築することができる。

【００２０】

外部記憶装置13には、ICカード22に、メッセージに対するデジタル署名の生成を依頼し、メッセージにICカード22により生成されたデジタル署名を付して、デジタル署名付きメッセージとして配布するための署名付きメッセージ作成PG（プログラム）131と、自デジタル署名者側装置1が作成したデジタル署名付きメッセージの検証をデジタル署名検証者側装置5に依頼したり、デジタル署名検証者側装置5からの指示にしたがい、当該デジタル署名検証者側装置5がデジタル署名付きメッセージの検証を行うのに必要な情報を当該デジタル署名検証者側装置5に提供するための検証依頼PG（プログラム）132が格納されている。これらのプログラムは、読取り装置14によりCD-ROMやFDなどの可搬性の記憶媒体15から読取られ、外部記憶装置13にインストールされるようにしてもよいし、あるいは、通信装置18を介してネットワークから外部記憶装置13にダウンロードされるようにしてもよい。

【００２１】

CPU11は、署名付きメッセージ作成PG131や検証依頼PG132をRAM12上にロードして実行することで、署名付きメッセージ作成処理部111や検証依頼処理部112をプロセスとして具現化する。

【００２２】

図３は、図２に示すICカード22の概略構成図である。

【００２３】

図示するように、ICカード22は、CPU221と、CPU221のワークエリアとして機能するRAM222と、各種プログラムやデータを記憶するEEPROM223と、ICカード接続装置19を介して電子計算機21と通信を行うI/O224とを有する。

【００２４】

EEPROM223には、署名付きメッセージ作成処理部111からの指示にしたがい、メッセージに対するデジタル署名を生成するための署名生成PG（プログラム）2231と、デジタル署名生成の際に用いる秘密鍵2232と、秘密鍵2232と対の公開鍵を含んだ公開鍵証明書2233と、デジタル署名生成の履歴を記録するための署名ログテーブル2234が格納されている。ここで、署名生成PG2231と秘密鍵2232は、ICカード22の発行時に設定され、ICカード22の外部からは読み出すことができないように設定されている。公開鍵証明書2233は、ICカード22の発行時に設定され、ICカード22の外部からも読み出すことができるように設定されている。また、署名ログテーブル2234は、ICカード22の発行時には何ら記録されておらず、ICカード22がデジタル署名を生成する毎に、生成されたデジタル署名と当該署名対象メッセージのハッシュ値と当該署名対象メッセージの購入者名（購入者側装置3のアドレスなど）でなる署名ログ2235が追記される。この署名ログテーブル2234は、ICカード22の外部から読み出すことは可能であるが、ICカード22の外部から書き換えることができないように、またデータを消去することができないように、設定されている。図３に示す例では、ICカード22でN回のデジタル署名生成処理が行われた後の状態を示しており、署名ログテーブル2234には、N個の署名ログ2235が記憶されている。なお、ICカード22の発行処理、すなわち、ICカード22のEEPROM223に、署名生成PG2231と秘密鍵2232と公開鍵証明書2233を格納・設定する処理は、ICカード発行業者が行うようにしてもよい。あるいは、ICカード発行業者は、ICカード22のEEPROM223に署名生成PG2231のみを格納した状態で発行し、ICカード22の所有者であるデジタル署名者が、秘密鍵2232と公開鍵証明書2233を、EEPROM223に格納・設定するようにしてもよい。

【００２５】

CPU221は、署名生成PG2231をRAM222上にロードして実行することで、署名生成

処理部2211をプロセスとして具現化する。

【００２６】

図４は、購入者側装置3の概略構成図である。

【００２７】

図示するように、購入者側装置3は、CPU31と、CPU31のワークエリアとして機能するRAM32と、ハードディスク装置などの外部記憶装置33と、CD-ROMやFDなどの可搬性を有する記憶媒体35からデータを読取る読取り装置34と、キーボードやマウスなどの入力装置36と、ディスプレイなどの表示装置37と、ネットワークを介して他の装置と通信を行うための通信装置38と、上述した各構成要素間のデータ送受を司るインターフェース40を備えた、一般的な構成を有する電子計算機41上に構築することができる。

【００２８】

外部記憶装置33には、デジタル署名側装置1からデジタル署名付きメッセージを入手するための署名付きメッセージ入手PG（プログラム）331と、入手したデジタル署名付きメッセージの検証をデジタル署名検証者側装置5に依頼するための検証依頼PG（プログラム）332が格納されている。これらのプログラムは、読取り装置34によりCD-ROMやFDなどの可搬性の記憶媒体35から読取られ、外部記憶装置33にインストールされるようにしてもよいし、あるいは、通信装置38を介してネットワークから外部記憶装置33にダウンロードされるようにしてもよい。

【００２９】

CPU31は、たとえば入力装置36に入力されたユーザの指示にしたがい、署名付きメッセージ入手PG331や検証依頼PG332をRAM32上にロードして実行する。これにより、署名付きメッセージ入手処理部311や検証依頼処理部312をプロセスとして具現化する。

【００３０】

なお、仲介者側装置7は、上述したように、購入者側装置3に代わってデジタル署名付きメッセージをデジタル署名者側装置1より入手する。基本的に、図４に示す購入者装置3と同様の構成を有する。

【００３１】

図５は、デジタル署名検証者側装置5の概略構成図である。

【００３２】

図示するように、デジタル署名検証者側装置5は、CPU51と、CPU51のワークエリアとして機能するRAM52と、ハードディスク装置などの外部記憶装置53と、CD-ROMやFDなどの可搬性を有する記憶媒体55からデータを読取る読取り装置54と、キーボードやマウスなどの入力装置56と、ディスプレイなどの表示装置57と、ネットワークを介して他の装置と通信を行うための通信装置58と、上述した各構成要素間のデータ送受を司るインターフェース60を備えた、一般的な構成を有する電子計算機61上に構築することができる。

【００３３】

外部記憶装置53には、デジタル署名者側装置1あるいは購入者側装置3からの指示にしたがい、デジタル署名付きメッセージの検証を行う署名検証PG（プログラム）531が格納されている。この署名検証PG531は、読取り装置54によりCD-ROMやFDなどの可搬性の記憶媒体55から読取られ、外部記憶装置53にインストールされるようにしてもよいし、あるいは、通信装置58を介してネットワークから外部記憶装置53にダウンロードされるようにしてもよい。

【００３４】

CPU51は、署名検証PG531をRAM52上にロードして実行することにより、署名検証処理部511をプロセスとして具現化する。

【００３５】

次に、上記構成のシステムの動作について説明する。

【００３６】

まず、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作について説明する。

【００３７】

図６は、本発明の第１実施形態において、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作を説明するためのフロー図である。

【００３８】

デジタル署名者側装置1において、署名付きメッセージ作成処理部111は、購入者側装置3よりメッセージの送信要求を受け取ると、その送信要求の対象であるメッセージを、たとえば各種メッセージが格納された外部記憶装置13から読み出し、これをハッシュ関数で評価することによりハッシュ値を求める。そして、メッセージのハッシュ値と送信要求を行った購入者側装置3のアドレスを署名生成処理部2211に送って署名生成を依頼する（ステップS6101）。これを受けて、署名生成処理部2211は、署名付きメッセージ作成処理部111より送られてきたメッセージのハッシュ値に、EEPROM223内に格納してある秘密鍵2232を作用させ、その結果をメッセージに対するデジタル署名とする（ステップS6102）。そして、署名生成処理部2211は、メッセージのハッシュ値とデジタル署名と送信要求を行った購入者側装置３のアドレスからなる署名ログ2235を、署名ログテーブル2234に登録する（ステップS6103）。それから、デジタル署名とEEPROM223内に格納してある公開鍵証明書2233を、署名付きメッセージ作成処理部111に送る。署名付きメッセージ作成処理部111は、送信要求の対象であるメッセージに署名生成処理部2211より送られてきたデジタル署名を付してデジタル署名付きメッセージを作成し、これに公開鍵証明書2233を添付して、送信要求を行った購入者側装置３に送信する（ステップS6104）。

【００３９】

一方、購入者側装置3において、署名付きメッセージ入手処理部311は、入力装置36を介して購入者よりメッセージ入手要求が指示されると、当該メッセージを保持する入手先のデジタル署名者側装置1へメッセージ送信要求を送信し（ステップS6001）、当該デジタル署名者側装置1からデジタル署名付きメッセージが送られてくるのを待つ（ステップS6002）。それから、署名付きメッセージ入手処理部311は、受け取ったデジタル署名付きメッセージに含まれるデジタル署名の検証を行う（ステップS6003）。具体的には、当該デジタル署名付きメッセージに含まれるデジタル署名に、当該デジタル署名付きメッセージに添付された公開鍵証明書2233の公開鍵を作用させる。そして、その結果を、当該デジタル署名付きメッセージに含まれるメッセージをハッシュ関数で評価することにより求めた

ハッシュ値と比較する。両者が一致する場合（ステップS6004でOKの場合）は、当該デジタル署名付きメッセージに含まれるデジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものであると認証し、当該デジタル署名付きメッセージを受け入れ、入手先のデジタル署名者側装置1のアドレスを付して外部記憶装置33などに格納する（ステップS6005）。一方、両者が一致しない場合（ステップS6004でNGの場合）は、当該デジタル署名付きメッセージを破棄する（ステップS6006）。

【００４０】

なお、上記では、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを直接入手する場合について説明したが、仲介者側装置7が購入者側装置3を代行する場合は、図６に示す購入者側装置3のフローを仲介者側装置7が実行し、ステップS6005で受け入れた署名付きメッセージを購入者側装置3に送信することで実現される。この場合、購入者側装置3は、ステップS6003に示す検証処理を行わなくてすむので、購入者側装置3の負担を軽減できる。なお、仲介者側装置7は、各デジタル署名者側装置１が所有するメッセージに関する情報を予め入手し、各デジタル署名者側装置１が所有するメッセージのリストをWebなどを用いて各購入者側装置３に公開しておくことが好ましい。

【００４１】

また、上記では、デジタル署名者側装置1は、購入者側装置3からの依頼を受けて、デジタル署名付きメッセージを作成する場合について説明しているが、デジタル署名者側装置1は、購入者側装置3からの依頼の有無にかかわらず、デジタル署名者の意思に基づいてデジタル署名付きメッセージを作成するよう変更してもかまわない。この場合、図６に示す購入者側装置3のフローは行われないことになる。しかし、デジタル署名付きメッセージの購入者は、購入者側装置3を用いて、後述する署名検証依頼をデジタル署名検証者側装置5に依頼することで、署名を検証することができる。

【００４２】

たとえば、メッセージが有価証券と同じ価値を持つデジタルデータ（ここでは、電子証券と呼ぶこととする）を例にとり説明すると、電子証券の発行者である

デジタル署名者は、デジタル署名者側装置1を用いて、図６に示すデジタル署名側装置1のフローを実行し、署名付き電子証券を作成・発行する。なお、電子証券の発行段階では、作成した署名付き電子証券の購入先が明らかでないので、署名ログテーブル2234に登録する署名ログ2235に購入先のアドレスは含まれない。

【００４３】

仲介者側装置７は、デジタル署名者側装置1が発行した署名付き電子証券を入手し、Webなどを用いて公開しておく。そして、購入者側装置３からの要求に応じて所望の署名付き電子証券を送信あるいは郵送等により送付する。電子証券の購入希望者は、実際に購入手続きを行う前に、購入者側装置3を用いて、購入予定の電子証券の検証をデジタル署名検証者側装置5に依頼し、有効性が確認された場合にだけ、実際の購入手続きを行うようにすることができる。

【００４４】

次に、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【００４５】

図７は、本発明の第１実施形態において、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【００４６】

購入者側装置3において、検証依頼処理部312は、入力装置36を介して購入者より、自装置が保持しているデジタル署名付きメッセージの検証要求が指示されると、当該デジタル署名付きメッセージに当該デジタル署名付きメッセージの入手先であるデジタル署名者側装置1のアドレスを付して、デジタル署名検証者側装置5に送信し、検証を依頼する（ステップS7001）。それから、デジタル署名検証者側装置5から検証結果が送られてくるのを待ち（ステップS7002）、検証結果をたとえば表示装置37に表示する（ステップS7003）。

【００４７】

一方、デジタル署名検証側装置5において、署名検証処理部511は、購入者側装

置3よりデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたデジタル署名付きメッセージに対し、第１段階の検証を行う（ステップS7101）。

【００４８】

具体的には、当該デジタル署名付きメッセージに含まれるデジタル署名に、当該デジタル署名付きメッセージに添付された公開鍵証明書2233の公開鍵を作用させる。そして、その結果と当該デジタル署名付きメッセージに含まれるメッセージをハッシュ関数で評価することにより求めたハッシュ値とを比較する。両者が一致する場合（ステップS7102でOKの場合）は、当該デジタル署名付きメッセージに含まれるデジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものであると認証し、ステップS7103に進む。一方、両者が一致しない場合（ステップS7102でNGの場合）は、当該デジタル署名付きメッセージに含まれるデジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものでない認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS7108）。

【００４９】

ステップS7103では、署名検証処理部511は、デジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に、署名ログテーブル2234に記録された全ての署名ログ2235（署名ログリストと称する）の送信を要求し（ステップS7103）、当該デジタル署名者側装置1から署名ログリストが送られてくるのを待つ（ステップS7104）。それから、署名検証処理部511は、デジタル署名付きメッセージに対し第２段階の検証を行う（ステップS7105）。

【００５０】

具体的には、デジタル署名付きメッセージに含まれるデジタル署名とステップS7101で求めたメッセージのハッシュ値を含む署名ログが、入手した署名ログリスト中に登録されているか否かを調べる。登録されている場合（ステップS7106でOKの場合）は、当該デジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成された正当なものであると認証し、その結果を

検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS7107）。一方、登録されていない場合（ステップS7106でNGの場合）、当該デジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成されていないと認定し、つまり、何らかの方法により秘密鍵2232を取得した第３者がデジタル署名者になりすまして、不当に生成したものと認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS7108）。

【００５１】

一方、デジタル署名者側装置1において、検証依頼処理部112は、デジタル署名検証者側装置5から、署名ログリストの送信要求や検証結果が送られてくるのを待つ（ステップS7201、S7203）。署名ログリストの送信要求が送られてきた場合は、EEPROM223の署名ログテーブル2234に登録されているすべての署名ログ2235を読み出して、デジタル署名検証者側装置5に送信する（ステップS7202）。検証結果が送られてきた場合は、その内容をたとえば表示装置17に表示する（ステップS7204）。このように、デジタル署名者者側装置1にも検証結果を伝えることで、たとえば、検証結果が、何らかの方法により秘密鍵2232を取得した第３者がデジタル署名者になりすまして不当にデジタル署名を生成していることを示している場合に、署名生成のための秘密鍵2232を変えるなどの対策を講じることが可能となる。

【００５２】

なお、上記のフローにおいて、デジタル署名者側装置1からデジタル署名検証者側装置5への履歴ログリストの送付は、上記のように、ネットワークを用いて通信により行う他、たとえば郵送などのよりICカード22自体を送付することにより行うようにしてもよい。

【００５３】

次に、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【００５４】

図８は、本発明の第１実施形態において、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【００５５】

デジタル署名者側装置1において、検証依頼処理部112は、入力装置16を介してデジタル署名者より、デジタル署名付きメッセージの購入者である購入者側装置3のアドレスが入力され、当該デジタル署名付きメッセージの検証要求が指示されると、入力された購入者側装置3のアドレスをデジタル署名検証者側装置5に送信し、検証を依頼する（ステップS8001）。その後、ステップS8002に進み、図７に示すフローのステップS7201～S7204の処理を実行する。

【００５６】

一方、デジタル署名検証側装置5において、署名検証処理部511は、デジタル署名者側装置1よりデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたアドレスにより特定される購入者側装置3に対し、検証要求を送信したデジタル署名者側装置1のアドレスを付したデジタル署名付きメッセージの送信を要求し（ステップS8101）、当該メッセージが送られてくるのを待つ（ステップS8102）。その後、ステップS8103に進み、図７に示すフローのステップS7101～S7109の処理を実行する。

【００５７】

一方、購入者側装置3において、検証依頼処理部312は、デジタル署名検証者側装置5よりデジタル署名付きメッセージの送信要求が送られてくるのを待つ（ステップS8201）。そして、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1より入手したデジタル署名付きメッセージを、たとえば外部記憶装置33などから読み出して、デジタル署名検証者側装置5に送信する（ステップS8202）。その後、ステップS8203に進み、図７に示すフローのステップS7002～S7003の処理を実行する。

【００５８】

以上、本発明の第１実施形態について説明した。

【００５９】

本実施形態によれば、デジタル署名者側装置1は、自らが生成したデジタル署名とメッセージを含むデジタル署名付きメッセージの配布に先立ち、当該デジタル署名とメッセージのハッシュ値を含む署名ログ2235を署名ログテーブル2234に登録する。

【００６０】

このようにすることで、デジタル署名検証者側装置5は、デジタル署名生成者者側装置１から署名ログテーブル2234に登録された全ての署名ログ2235でなる署名ログリストを入手し、検証すべきデジタル署名付きメッセージに含まれるメッセージのハッシュ値とデジタル署名を含む署名ログが当該署名ログリストに登録されているか否かを調べることで、当該検証すべきデジタル署名付きメッセージがデジタル署名者側装置1により生成された正当なものであるか、それとも、何らかの方法により秘密鍵2232を取得した第３者がデジタル署名者になりすまして不正に生成したものであるかを識別することが可能となる。

【００６１】

なお、上記の実施形態では、デジタル署名者側装置１において、署名ログテーブル2234をICカード22内のEEPROM223に設定している。しかしながら、本発明はこれに限定されない。

【００６２】

たとえば、ICカード22内のEEPROM223に加えて、電子計算機21が備える外部記憶装置13にも署名ログテーブルを設定するようにしてもよい。そして、EEPROM223の署名ログテーブルに新たに生成した署名ログを登録する場合に、当該ログを登録することで、EEPROM223の署名ログテーブルに登録されるログ数が所定数（この数はEEPROM223の容量を考慮して設定すればよい）を超える場合は、EEPROM223の署名ログテーブルに登録されている署名ログのうち最も古いログを電子計算機21に出力して、外部記憶装置13の署名ログテーブルに登録するとともに、当該最も古いログをEEPROM223の署名ログテーブルから削除してから、前記新たに生成した署名ログをEEPROM223の署名ログテーブルに登録するようにしてもよい。あるいは、新たに生成した署名ログを、ICカード22のEEPROM223の署名ログテー

ブルおよび電子計算機21の外部記憶装置13の署名ログテーブル各々に登録するとともに、前記新たに生成した署名ログをICカード22のEEPROM223の署名ログテーブルに登録することで、EEPROM223の署名ログテーブルに登録されるログ数が所定数を超える場合は、EEPROM223の署名ログテーブルに登録されている署名ログのうち最も古いログをEEPROM223の署名ログテーブルから削除してから、前記新たに生成した署名ログをICカード22のEEPROM223の署名ログテーブルに登録するようにしてもよい。このようにすることで、ICカード22内のEEPROM223の容量が小さい場合でも、デジタル署名者側装置１を実現することが可能となる。なお、この場合、外部記憶装置13に設定される署名ログテーブルは、デジタル署名者が署名ログを改竄するのを防ぐため、ICカード22からのみ書き込み可能に設定するか、または、CD-Rなどの書き換え不可の記憶媒体を用いることが好ましい。

【００６３】

また、ICカード22内のEEPROM223に署名ログテーブルを設定する代わりに、図９に示すように、各デジタル署名者側装置1毎に署名ログテーブルを管理する署名ログ管理装置9を設けるようにしてもよい。そして、デジタル署名者側装置1は、新たにデジタル署名を生成する毎に、署名ログを署名ログ管理装置9の自デジタル署名者側装置1に対応付けて設けられた署名ログテーブルに登録するようにしてもよい。この場合、図７に示すフローのステップS7103において、デジタル署名検証者側装置5は、署名ログ管理装置９に対し、署名ログリストの送信要求を、検証対象デジタル署名付きメッセージを作成したデジタル署名者側装置1のアドレスを付して行う。また、図７に示すフローのステップS7201、S7202は署名ログ管理装置9が行う。署名ログ管理装置9は、署名ログリストの送信要求を受けた場合に、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1の署名ログリストをデジタル署名検証者側装置5に送信する。このようにすることで、デジタル署名者による署名ログの改竄を防止することができる。なお、署名ログ管理装置９は、デジタル署名検証者側装置5と同じ電子計算機上に構築されるようにしてもかまわない。

【００６４】

次に、本発明の第２実施形態について説明する。

【００６５】

本実施形態は、上記の第１実施形態において、デジタル署名者による署名ログの改竄をより効果的に防止できるようにしたものである。なお、本実施形態にかかるシステムの各装置の構成は、署名ログテーブル2234に格納される署名ログ2235の構成を除けば、基本的に第１実施形態のものと同様である。そこで、本実施形態では、システムの動作についてのみ説明する。

【００６６】

まず、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作について説明する。

【００６７】

この動作は、図６に示す第１実施形態のものと同様である。しかしながら、デジタル署名者側装置1における署名生成の具体的な処理内容と、購入者装置3における署名検証の具体的な処理内容が異なる。

【００６８】

すなわち、デジタル署名者側装置1において、署名付きメッセージ作成処理部111は、購入者側装置3よりメッセージの送信要求を受け取ると、その送信要求の対象であるメッセージを読み出し、これをハッシュ関数で評価することによりハッシュ値を求める。そして、メッセージのハッシュ値と送信要求を行った購入者側装置3のアドレスを署名生成処理部2211に送って署名生成を依頼する（ステップS6101）。これを受けて、署名生成処理部2211は、前回の署名生成処理により署名ログテーブル2234に格納した署名ログ2235に含まれるメッセージのハッシュ値およびデジタル署名（これを前データと称する）と、署名付きメッセージ作成処理部111より送られてきたメッセージのハッシュ値とに、EEPROM223内に格納してある秘密鍵2232を作用させ、その結果をメッセージに対するデジタル署名とする（ステップS6102）。そして、署名生成処理部2211は、前データとメッセージのハッシュ値とデジタル署名と送信要求を行った購入者側装置３のアドレスからなる署名ログ2235を、署名ログテーブル2234に登録する（ステップS6103）。それから、前データとデジタル署名とEEPROM223内に格納してある公開鍵証明書2233を、署名付きメッセージ作成処理部111に送る。署名付きメッセージ作成処理部

111は、送信要求の対象であるメッセージに前データとデジタル署名を付してデジタル署名付きメッセージを作成し、これに公開鍵証明書2233を添付して、送信要求を行った購入者側装置３に送信する（ステップS6104）。

【００６９】

上記の処理により、署名ログテーブル2234に格納される署名ログ2235は、図１０に示すように、前データ（前回の署名生成処理により署名ログテーブル2234に登録された署名ログ2235に含まれるメッセージのハッシュ値およびデジタル署名）とメッセージのハッシュ値とデジタル署名を含んで構成されることになる。

【００７０】

一方、購入者側装置3において、署名付きメッセージ入手処理部311は、入力装置36を介して購入者よりメッセージ入手要求が指示されると、当該メッセージを保持する入手先のデジタル署名者側装置1へメッセージ送信要求を送信し（ステップS6001）、当該デジタル署名者側装置1からデジタル署名付きメッセージが送られてくるのを待つ（ステップS6002）。それから、署名付きメッセージ入手処理部311は、受け取ったデジタル署名付きメッセージに含まれるデジタル署名の検証を行う（ステップS6003）。具体的には、当該デジタル署名付きメッセージに含まれるデジタル署名に、当該デジタル署名付きメッセージに添付された公開鍵証明書2233の公開鍵を作用させる。そして、その結果を、当該デジタル署名付きメッセージに含まれる前データと当該デジタル署名付きメッセージに含まれるメッセージをハッシュ関数で評価することにより求めたハッシュ値の組と比較する。両者が一致する場合（ステップS6004でOKの場合）は、当該デジタル署名付きメッセージに含まれるデジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものであると認証し、当該デジタル署名付きメッセージを受け入れ、入手先のデジタル署名者側装置1のアドレスを付して外部記憶装置33などに格納する（ステップS6005）。一方、両者が一致しない場合（ステップS6004でNGの場合）は、当該デジタル署名付きメッセージを破棄する（ステップS6006）。

【００７１】

次に、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者

側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【００７２】

図１１は、本発明の第２実施形態において、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【００７３】

購入者側装置3において、検証依頼処理部312は、入力装置36を介して購入者より、自装置が保持しているデジタル署名付きメッセージの検証要求が指示されると、検証対象のデジタル署名付きメッセージに当該デジタル署名付きメッセージの入手先であるデジタル署名者側装置1のアドレスを付して、デジタル署名検証者側装置5に送信し、検証を依頼する（ステップS11001）。それから、デジタル署名検証者側装置5から検証結果が送られてくるのを待ち（ステップS11002）、検証結果をたとえば表示装置37に表示する（ステップS11003）。

【００７４】

また、検証依頼処理部312は、デジタル署名検証者側装置5より、デジタル署名付きメッセージを参考資料として送信する旨の要求が送られてくると（ステップS11101）、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1より入手したデジタル署名付きメッセージを、たとえば外部記憶装置33などから読み出して、デジタル署名検証者側装置5に送信する（ステップS11102）。

【００７５】

一方、デジタル署名検証側装置5において、署名検証処理部511は、購入者側装置3よりデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきた検証対象のデジタル署名付きメッセージに対し、第１段階の検証を行う（ステップS11201）。

【００７６】

具体的には、当該デジタル署名付きメッセージに含まれるデジタル署名に、当該デジタル署名付きメッセージに添付された公開鍵証明書2233の公開鍵を作用させる。そして、その結果を、当該デジタル署名付きメッセージに含まれる前デー

タと当該デジタル署名付きメッセージに含まれるメッセージをハッシュ関数で評価することにより求めたハッシュ値の組と比較する。両者が一致する場合（ステップS11202でOKの場合）は、当該デジタル署名付きメッセージに含まれるデジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものであると認証し、ステップS11203に進む。一方、両者が一致しない場合（ステップS11202でNGの場合）は、当該デジタル署名付きメッセージに含まれるデジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものでない認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS11214）。

【００７７】

ステップS11203では、署名検証処理部511は、デジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に、署名ログリストの送信を要求し、当該デジタル署名者側装置1から署名ログリストが送られてくるのを待つ（ステップS11204）。それから、署名検証処理部511は、デジタル署名付きメッセージに対し第２段階の検証を行う（ステップS11205）。

【００７８】

具体的には、デジタル署名付きメッセージに含まれるデジタル署名および前データとステップS11201で求めたメッセージのハッシュ値とを含む署名ログが、入手した署名ログリストに登録されているか否かを調べる。登録されている場合（ステップS11206でOKの場合）は、当該デジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成されたものであると認証し、ステップS11207に進む。一方、登録されていない場合（ステップS11206でNGの場合）、当該デジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成されていないと認定し、つまり、何らかの方法により秘密鍵2232を取得した第３者がデジタル署名者になりすまして、不当に生成したものと認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS11215）。

【００７９】

ステップS11207では、署名検証処理部511は、デジタル署名付きメッセージに対し第３段階の検証を行う（ステップS11205）。

【００８０】

具体的には、ステップS11204で入手した署名ログリストにおいて、検証対象のデジタル署名付きメッセージに対応する署名ログよりも、１つ前に登録されている署名ログに含まれるメッセージのハッシュ値とデジタル署名を読み出す。たとえば、図１０において、検証対象のデジタル署名付きメッセージに含まれるデジタル署名および前データとステップS11201で求めたメッセージのハッシュ値とを含む署名ログがN番目である場合、N-1番目の署名ログに含まれるメッセージのハッシュ値とデジタル署名を読み出す。それから、署名検証処理部511は、１つ前に登録されている署名ログに含まれるメッセージのハッシュ値とデジタル署名を、検証対象のデジタル署名付きメッセージに含まれる前データと比較する。ここで、前データは、上述したように、１つ前に登録されている署名ログに含まれるメッセージのハッシュ値とデジタル署名で構成される。したがって、両者が一致しない場合（ステップS11208でNGの場合）は、検証対象のデジタル署名付きメッセージに対応する署名ログが改竄されたものと認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS11216）。一方、両者が一致する場合（ステップS11206でOKの場合）は、ステップS11209に進む。

【００８１】

ステップS11209では、ステップS11204で入手した署名ログリストにおいて、検証対象のデジタル署名付きメッセージに対応する署名ログよりも１つ前に登録されている署名ログに含まれる購入者のアドレスにより特定される購入者側装置3に対し、デジタル署名付きメッセージを参考資料として送信すべき旨の要求を、検証要求を送信したデジタル署名者側装置1のアドレスを付して行い、当該メッセージが送られてくるのを待つ（ステップS11210）。それから、署名検証処理部511は、デジタル署名付きメッセージに対し第４段階の検証を行う（ステップS11211）。

【００８２】

具体的には、ステップS11210で入手したデジタル署名付きメッセージに含まれるメッセージをハッシュ関数で評価することで、当該メッセージのハッシュ値を求める。そして、ステップS11210で入手したデジタル署名付きメッセージに含まれるデジタル署名および前データと当該メッセージのハッシュ値が、ステップS11204で入手した署名ログリストにおいて、検証対象のデジタル署名付きメッセージに対応する署名ログよりも１つ前に登録されている署名ログの内容と一致するか否かを調べる。両者が一致しない場合は、検証対象のデジタル署名付きメッセージに対応する署名ログとこれより１つ前に記録されている参考資料のデジタル署名付きメッセージに対応する署名ログの両方が改竄され、その結果、ステップS11208における第３段階の検証の結果がOKとされた可能性がある。そこで、両者が一致しない場合（ステップS11212でNGの場合）は、検証対象のデジタル署名付きメッセージに対応する署名ログが改竄された可能性があると認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS11216）。一方、両者が一致する場合（ステップS11212でOKの場合）、検証対象のデジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成された正当なものであると認証し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS11213）。

【００８３】

一方、デジタル署名者側装置1において、検証依頼処理部112は、デジタル署名検証者側装置5から、署名ログリストの送信要求や検証結果が送られてくるのを待つ（ステップS11301、S11303）。署名ログリストの送信要求が送られてきた場合は、署名ログテーブル2234に登録されている全ての署名ログ2235を読み出して、デジタル署名検証者側装置5に送信する（ステップS11302)。検証結果が送られてきた場合は、その内容をたとえば表示装置17に表示する（ステップS11305）。

【００８４】

なお、上記のフローにおいて、デジタル署名者側装置1からデジタル署名検証

者側装置5への履歴ログリストの送付は、上記のようにネットワークを用いて通信により行う他、たとえば郵送などのよりICカード22自体を送付することにより行うようにしてもよい。

【００８５】

次に、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【００８６】

図１２は、本発明の第２実施形態において、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【００８７】

デジタル署名者側装置1において、検証依頼処理部112は、入力装置16を介してデジタル署名者より、デジタル署名付きメッセージの購入者である購入者側装置3のアドレスが入力され、当該デジタル署名付きメッセージの検証要求が指示されると、入力された購入者側装置3のアドレスをデジタル署名検証者側装置5に送信し、検証を依頼する（ステップS12001）。その後、ステップS12002に進み、図１１に示すフローのステップS11301～S11305の処理を実行する。

【００８８】

一方、デジタル署名検証側装置5において、署名検証処理部511は、デジタル署名者側装置1よりデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたアドレスにより特定される購入者側装置3に対し、検証対象のデジタル署名付きメッセージを送信すべき旨の要求を、検証要求を送信したデジタル署名者側装置1のアドレスを付して行い（ステップS12101）、当該メッセージが送られてくるのを待つ（ステップS12102）。その後、ステップS12103に進み、図１１に示すフローのステップS11201～S11217の処理を実行する。

【００８９】

一方、購入者側装置3において、検証依頼処理部312は、デジタル署名検証者側装置5より、検証対象のデジタル署名付きメッセージの送信要求が送られてくる

と（ステップS12201）、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1より入手した検証対象のデジタル署名付きメッセージを読み出して、デジタル署名検証者側装置5に送信する（ステップS12203）。その後、ステップS12204に進み、図１１に示すフローのステップS11002～S11003の処理を実行する。また、検証依頼処理部312は、デジタル署名検証者側装置5より、参考資料としてのデジタル署名付きメッセージの送信要求が送られてくると（ステップS12202）、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1より入手した参考資料としてのデジタル署名付きメッセージを読み出して、デジタル署名検証者側装置5に送信する（ステップS12205）。

【００９０】

以上、本発明の第２実施形態について説明した。

【００９１】

本実施形態によれば、デジタル署名者側装置1は、署名対象となるメッセージのハッシュ値と、署名ログテーブル2234に登録されている最新の署名ログ（つまり、1つ前に生成したデジタル署名付きメッセージに対応する署名ログ）に含まれるデジタル署名およびメッセージのハッシュ値（前データ）とに、秘密鍵2232を作用させることで、署名対象メッセージに対するデジタル署名を生成する。そして、署名対象メッセージに前データとデジタル署名を付してデジタル署名付きメッセージを作成し配布するとともに、デジタル署名とメッセージのハッシュ値と前データを含む署名ログを署名ログテーブル2234に登録する。

【００９２】

このようにすることで、検証対象のデジタル署名付きメッセージに含まれる前データが、署名ログテーブル2234において、当該デジタル署名付きメッセージに対応する署名ログより１つ前に登録されている署名ログに含まれるデジタル署名およびメッセージのハッシュ値と一致するか否かを調べることで、署名ログになされた改竄を検出することが可能となる。

【００９３】

さらに、検証対象のデジタル署名付きメッセージに含まれる前データが、署名ログテーブル2234において、当該デジタル署名付きメッセージに対応する署名ロ

グより１つ前に登録されている署名ログに含まれるデジタル署名およびメッセージのハッシュ値と一致する場合に、前記１つ前に登録されている署名ログに対応するデジタル署名付きメッセージを入手して、当該デジタル署名付きメッセージに含まれるデジタル署名および前データと当該デジタル署名付きメッセージに含まれるメッセージのハッシュ値が、当該１つ前に登録されている署名ログの内容と一致するか否かを検証することで、デジタル署名付きメッセージの正当性をより詳しく調べることが可能となる。

【００９４】

なお、上記の実施形態では、デジタル署名検証者側装置5での第３段階の署名検証（図１１のステップS11207）において、検証対象のデジタル署名付きメッセージに含まれる前データが、署名ログテーブル2234において、当該デジタル署名付きメッセージに対応する署名ログより１つ前に登録されている署名ログに含まれるデジタル署名およびメッセージのハッシュ値と一致するか否かを調べることで、署名ログになされた改竄を検出している。しかし、第３段階での署名検証は、たとえば、以下のように修正することも可能である。

【００９５】

すなわち、署名ログテーブル2234に記録されている全ての署名ログのうち、検証対象のデジタル署名付きメッセージに対応する署名ログを含む任意数の組について、当該署名ログに含まれる前データが、１つ前の署名ログに含まれるデジタル署名およびメッセージのハッシュ値と一致するか否かを調べることで署名ログの改竄を検出するようにしてもよい。

【００９６】

また、本実施形態においても、上記の第１実施形態と同様に、ICカード22内のEEPROM223に加えて、電子計算機21が備える外部記憶装置13にも署名ログテーブル2234を設定するようにしてもよい。あるいは、ICカード22内のEEPROM223に署名ログテーブル2234を設定する代わりに、図９に示すように、各デジタル署名者側装置1毎に署名ログテーブルを管理する署名ログ管理装置9を設けるようにしてもよい。さらには、この署名ログ管理装置9は、上記の第１実施形態と同様、デジタル署名検証者側装置5と同じ電子計算機上に構築されるようにしてもよい。

【００９７】

なお、署名ログ管理装置9を設ける場合、署名ログの署名ログリストへの登録に先立って、署名ログ管理装置9にて、図１１に示すフローのステップS11207、S11209（第３段階の署名検証）を行い、検証結果がOKの場合にのみ、当該署名ログの署名ログリストへの登録を認めるようにしてもい。すなわち、署名ログの署名ログリストへの登録に先立ち、当該署名ログに含まれる前データが、署名ログリストに登録されている最新の署名ログデータに含まれているメッセージのハッシュ値およびデジタル署名と一致する場合にのみ、当該署名ログの署名ログリストへの登録を許可するようにしてもよい。このようにすることで、デジタル署名検証者側装置5にて、図１１に示すフローのステップS11207、S11209（第３段階の署名検証）を省略することも可能である。

【００９８】

次に、本発明の第３実施形態について説明する。

【００９９】

本実施形態は、上記の第１実施形態において、デジタル署名に時刻情報を含めることで、当該時刻情報からもデジタル署名の有効・無効を判定できるようにしたものである。

【０１００】

図１３は本発明の第３実施形態が適用されたシステムの概略図である。

【０１０１】

図示するように、本システムは、図１に示す第１実施形態のシステムに、デジタル署名者側装置１から送られてきたデジタル署名に対してタイムスタンプを発行するタイムスタンプ発行装置8が追加された構成となっている。

【０１０２】

図１４は、タイムスタンプ発行装置8の概略構成図である。

【０１０３】

図示するように、タイムスタンプ発行装置8は、CPU81と、CPU81のワークエリアとして機能するRAM82と、ハードディスク装置などの外部記憶装置83と、CD-ROMやFDなどの可搬性を有する記憶媒体85からデータを読取る読取り装置84と、キ

ーボードやマウスなどの入力装置86と、ディスプレイなどの表示装置87と、ネットワークを介して他の装置と通信を行うための通信装置88と、上述した各構成要素間のデータ送受を司るインターフェース90を備えた、一般的な構成を有する電子計算機91上に構築することができる。

【０１０４】

外部記憶装置83には、デジタル署名者側装置１から送られてきたデジタル署名および時刻データを暗号化してタイムスタンプを生成するためのタイムスタンプ発行PG（プログラム）831と、タイムスタンプ生成の際に用いる秘密鍵832と、秘密鍵832と対の公開鍵を含んだ公開鍵証明書833が格納されている。ここで、タイムスタンプ発行PG831は、読取り装置84によりCD-ROMやFDなどの可搬性の記憶媒体85から読取られ、外部記憶装置83にインストールされるようにしてもよいし、あるいは、通信装置88を介してネットワークから外部記憶装置83にダウンロードされるようにしてもよい。

【０１０５】

CPU81は、タイムスタンプ発行PG831をRAM82上にロードして実行することで、タイムスタンプ発行処理部811をプロセスとして具現化する。

【０１０６】

次に、上記構成のシステムの動作について説明する。

【０１０７】

まず、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作について説明する。

【０１０８】

図１５は、本発明の第３実施形態において、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作を説明するためのフロー図である。

【０１０９】

デジタル署名者側装置1において、署名付きメッセージ作成処理部111は、購入者側装置3よりメッセージの送信要求を受け取ると、その送信要求の対象であるメッセージを読み出し、これをハッシュ関数で評価することによりハッシュ値を

求める。そして、メッセージのハッシュ値と送信要求を行った購入者側装置3のアドレスを署名生成処理部2211に送り、図６に示すステップS6101～S6103の処理を実行する（ステップS15101）。それから、署名付きメッセージ作成処理部111は、署名生成処理部2211から送られてきたデジタル署名を、タイムスタンプ発行装置8に送信して、タイムスタンプの発行を依頼する（ステップS15102）。署名付きメッセージ作成処理部111は、タイムスタンプ発行装置8よりタイムスタンプを受け取ると（ステップS15103）、送信要求の対象であるメッセージに当該タイムスタンプを付してデジタル署名付きメッセージを作成し、これに、署名生成処理部2211からデジタル署名とともに送られてきた公開鍵証明書2233と、タイムスタンプ発行装置8からタイムスタンプとともに送られてきた公開鍵証明書833を添付して、送信要求を行った購入者側装置３に送信する（ステップS15104）。

【０１１０】

一方、タイムスタンプ発行装置8において、タイムスタンプ発行処理部811は、デジタル署名者側装置1からデジタル署名が送られてくると、タイムスタンプを生成する（ステップS15201）。具体的には、デジタル署名者側装置1から送られてきたデジタル署名と当該デジタル署名の受信時刻を示す時刻データを、外部記憶装置83に格納してある秘密鍵832を用いて暗号化することで、タイムスタンプを生成する。それから、タイムスタンプ発行処理部811は、生成したタイムスタンプに、外部記憶装置83に格納してある公開鍵証明書833を付して、デジタル署名を送信したデジタル署名者側装置1に送信する（ステップS15202）。

【０１１１】

一方、購入者側装置3において、署名付きメッセージ入手処理部311は、入力装置36を介して購入者よりメッセージ入手要求が指示されると、図６に示すステップS6001～S6002の処理を実行し、デジタル署名付きメッセージを取得する（ステップS15001）。次に、署名付きメッセージ入手処理部311は、受け取ったデジタル署名付きメッセージに含まれるタイムスタンプを、当該メッセージに添付された公開鍵証明書821の公開鍵（タイムスタンプ発行装置8の公開鍵）を用いて復号化することで、デジタル署名を得る（ステップS15002）。それから、ステップS6004～S6006の処理を実行して、デジタル署名の検証を行う（ステップS15003）。

【０１１２】

次に、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【０１１３】

なお、本実施形態において、デジタル署名者側装置１の使用者であるデジタル署名者は、自身が秘密裏に保持する秘密鍵2232が暴露され、第３者が不正に入手した可能性がある場合、暴露の日時を指定して速やかにデジタル署名検証者に連絡するものとする。そして、デジタル署名検証者は、デジタル署名者が通知した日時と当該デジタル署名者が使用するデジタル署名者側装置１のアドレスとを対応付けて、デジタル署名検証者側装置5の外部記憶装置53に格納させることとする。

【０１１４】

図１６は、本発明の第３実施形態において、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【０１１５】

購入者側装置3において、検証依頼処理部312は、入力装置36を介して購入者より、自装置が保持しているデジタル署名付きメッセージの検証要求が指示されると、図７に示すフローのステップS7001～S7003の処理を実行し、デジタル署名検証者側装置5から検証結果を入手する（ステップS16001）。

【０１１６】

一方、デジタル署名検証側装置5において、署名検証処理部511は、購入者側装置3よりデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたデジタル署名付きメッセージに含まれるタイムスタンプを、当該デジタル署名付きメッセージに添付された公開鍵証明書821の公開鍵（タイムスタンプ発行装置8の公開鍵）を用いて復号化することで、時刻データとデジタル署名を得る（ステップS16101）。

【０１１７】

次に、署名検証処理部511は、外部記憶装置53を調べて、デジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に対して、秘密鍵2232の暴露日時が設定されているか否かを確認する（ステップS16102）。暴露日時が設定されている場合は、ステップS16103に進み、設定されていない場合は、ステップS16105に進んで、図７に示すステップS7101～S7109の処理を実行する。

【０１１８】

ステップS16103では、署名検証処理部511は、ステップS16101で得た時刻データが示す日時が外部記憶装置53に設定されている暴露時刻より新しいか否かを調べる（ステップS16103）。新しい場合は、検証対象のデジタル署名付きメッセージは無効であると判定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（ステップS16104）。一方、新しくない場合は、ステップS16105に進んで、図７に示すステップS7101～S7109の処理を実行する。

【０１１９】

一方、デジタル署名者側装置1において、検証依頼処理部112は、デジタル署名検証者側装置5から、署名ログリストの送信要求や検証結果が送られてくると、図７に示すステップS7201～S7204の処理を実行する（ステップS16201）。

【０１２０】

次に、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【０１２１】

図１７は、本発明の第３実施形態において、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【０１２２】

デジタル署名者側装置1において、検証依頼処理部112は、入力装置16を介して

デジタル署名者より、デジタル署名付きメッセージの購入者である購入者側装置3のアドレスが入力され、当該デジタル署名付きメッセージの検証要求が指示されると、図８に示すステップS8001～S8002の処理を実行し、検証結果を入手する（ステップS17201）。

【０１２３】

一方、デジタル署名検証側装置5において、署名検証処理部511は、デジタル署名者側装置1よりデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたアドレスにより特定される購入者側装置3に対し、検証要求を送信したデジタル署名者側装置1のアドレスを付したデジタル署名付きメッセージの送信を要求し（ステップS17101）、当該メッセージが送られてくるのを待つ（ステップS17102）。その後、ステップS17103に進み、図１６に示すステップS16101～S16105の処理を実行する。

【０１２４】

一方、購入者側装置3において、検証依頼処理部312は、デジタル署名検証者側装置5よりデジタル署名付きメッセージの送信要求が送られてくると、図８に示すステップS8201～S8203の処理を実行する（ステップS17001）。

【０１２５】

以上、本発明の第３実施形態について説明した。

【０１２６】

本実施形態によれば、デジタル署名検証者側装置３は、検証対象のデジタル署名付きメッセージに添付されたタイムスタンプ発行局側装置８の公開鍵証明書833の公開鍵を用いて、当該メッセージに含まれるタイムスタンプを復号化してデジタル署名と時刻データを取得し、この時刻データが示す日時が、デジタル署名生成者より通知された暴露日時を過ぎているか否かを調べるようにしている。このようにすることで、デジタル署名の検証に先立ち、当該デジタル署名の有効・無効を調べることができる。

【０１２７】

なお、上記の実施形態において、デジタル署名者側装置1は、デジタル署名を生成する毎に、当該デジタル署名をタイムスタンプ発行装置8に送信してタイム

スタンプの発行を依頼している。しかしながら、本発明はこれに限定されない。タイムスタンプの発行依頼は、間欠的（たとえば、m回に１回）に行うようにしてもよい。この場合、デジタル署名検証者側装置3において、タイムスタンプが付与されていないデジタル署名付きメッセージに対して、デジタル署名生成者より通知された暴露日時に基づいたデジタル署名の有効・無効を判定する場合には、以下のようにして行えばよい。

【０１２８】

すなわち、デジタル署名者側装置１は、デジタル署名をタイムスタンプ発行装置8に送信してタイムスタンプの発行を依頼した場合、図１８に示すように、タイムスタンプ発行装置8から送られてきたタイムスタンプを、当該スタンプの対象となるデジタル署名の署名ログ2235に含めて署名ログテーブル2234に登録する。なお、署名ログデーブル2234への登録は時系列的に行う。

【０１２９】

デジタル署名検証者側装置３は、署名ログテーブル2234において、検証対象のデジタル署名付きメッセージに対応する署名ログより前に登録されている署名ログであって、タイムスタンプが記録されている署名ログを検出し、当該タイムスタンプを復号化して時刻データを得る。署名ログデーブル2234への登録は、時系列的に行われているので、検証対象のデジタル署名付きメッセージは、少なくとも復号化された時刻データが示す日時より後に生成されたものである。したがって、デジタル署名者から通知された暴露日時がこの復号化された時刻データが示す日時より前である場合には、検証対象のデジタル署名付きメッセージは無効と判定する。

【０１３０】

また、上記の実施形態では、第１実施形態において、タイムスタンプによるデジタル署名の有効・無効を判定できるようにした場合について説明したが、当然のことながら、第２実施形態において、タイムスタンプによるデジタル署名の有効・無効を判定できるようすることも可能である。あるいは、第１実施形態や第２実施形態と組み合わせることなく、タイムスタンプによるデジタル署名の有効・無効を判定できるにすることも可能である。

【０１３１】

本発明は、上記の各実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【０１３２】

たとえば、上記の各実施形態では、署名ログ2235にメッセージのハッシュ値を含めるようにしているが、署名ログテーブル2234を格納する記憶装置の容量に余裕がある場合などにおいては、メッセージをそのものを署名ログ2235に含めるようにしてもよい。

【０１３３】

また、上記の各実施形態では、デジタル署名者側装置１を、電子計算機21とICカード22で構成し、デジタル署名の生成処理をICカード22内で行うようにしたものについて説明したが、本発明はこれに限定されない。デジタル署名者側装置１で行うべき全ての処理を電子計算機21内で行うようにしてもよい。

【０１３４】

また、上記の各実施形態では、デジタル署名検証者側装置5における第１段階の署名検証を、いわゆるRSA署名を適用した場合を例にとり説明しているが、本発明はこれに限定されない。デジタル署名と、メッセージ（第２実施形態ではこれに加えて前データ）と、デジタル署名者が所有する秘密鍵と対の公開鍵を用いて、前記デジタル署名が前記メッセージに対してなされたものであるか否かを認証することが可能な、様々な署名方法を適用できる。

【０１３５】

【発明の効果】

以上説明したように、本発明によれば、デジタル署名生成者自身がしたデジタル署名と第３者がデジタル署名生成者になりすまして行ったデジタル署名とを識別可能なデジタル署名技術を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態が適用されたシステムの概略図である。

【図２】

図１に示すデジタル署名者側装置1の概略構成図である。

【図３】

図２に示すICカード22の概略構成図である。

【図４】

図１に示す購入者側装置3の概略構成図である。

【図５】

図１に示すデジタル署名検証者側装置5の概略構成図である。

【図６】

本発明の第１実施形態において、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作を説明するためのフロー図である。

【図７】

本発明の第１実施形態において、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図８】

本発明の第１実施形態において、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図９】

本発明の第１実施形態が適用されたシステムの変形例を示す図である。

【図１０】

本発明の第２実施形態において、署名ログテーブル2234に格納されるデータの構成を説明するための図である。

【図１１】

本発明の第２実施形態において、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図１２】

本発明の第２実施形態において、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図１３】

本発明の第３実施形態が適用されたシステムの概略図である。

【図１４】

図１３に示すタイムスタンプ発行装置8の概略構成図である。

【図１５】

本発明の第３実施形態において、購入者側装置3がデジタル署名者側装置1よりデジタル署名付きメッセージを入手する際の動作を説明するためのフロー図である。

【図１６】

本発明の第３実施形態において、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1より入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図１７】

本発明の第３実施形態において、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図１８】

本発明の第３実施形態の変形例において、署名ログテーブル2234に格納されるデータの構成を説明するための図である。

【符号の説明】

1…デジタル署名者側装置

3…購入者側装置

5…デジタル署名検証者側装置

7…仲介者側装置

8…タイムスタンプ発行装置

9…署名ログ管理装置

11,31,51,81,221…CPU

12,32,52,82,222…RAM

13,33,53,83…外部記憶装置

14,34,54,84…読取り装置

15,35,55,85…記憶媒体

16,36,56,86…入力装置

17,37,57,87…表示装置

18,38,58,88…通信装置

19…ICカード接続装置

20,40,60,90…インターフェース

21,41,61,91…電子計算機

22…ICカード

111…署名付きメッセージ作成処理依頼部

112,312…検証依頼処理部

131…署名付きメッセージ作成プログラム

132,332…検証依頼プログラム

223…EEPROM

224…I/O

311…署名付きメッセージ入手処理部

331…署名付きメッセージ入手プログラム

511…署名検証処理部

531…署名検証プログラム

811…タイムスタンプ発行処理部

831…タイムスタンプ発行プログラム

832,2232…秘密鍵

833,2233…公開鍵証明書

2211…署名生成処理部

2231…署名生成プログラム

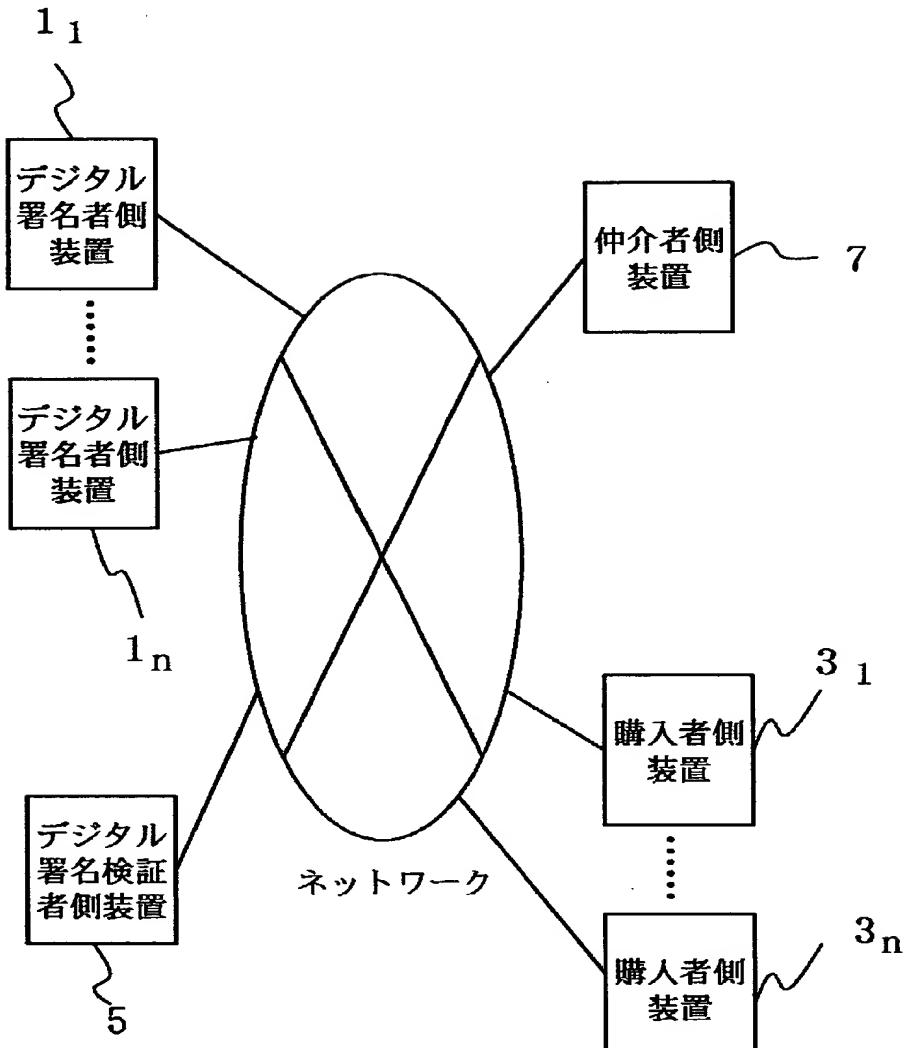
2234…署名ログテーブル

2235…署名ログ

【書類名】図面

【図１】

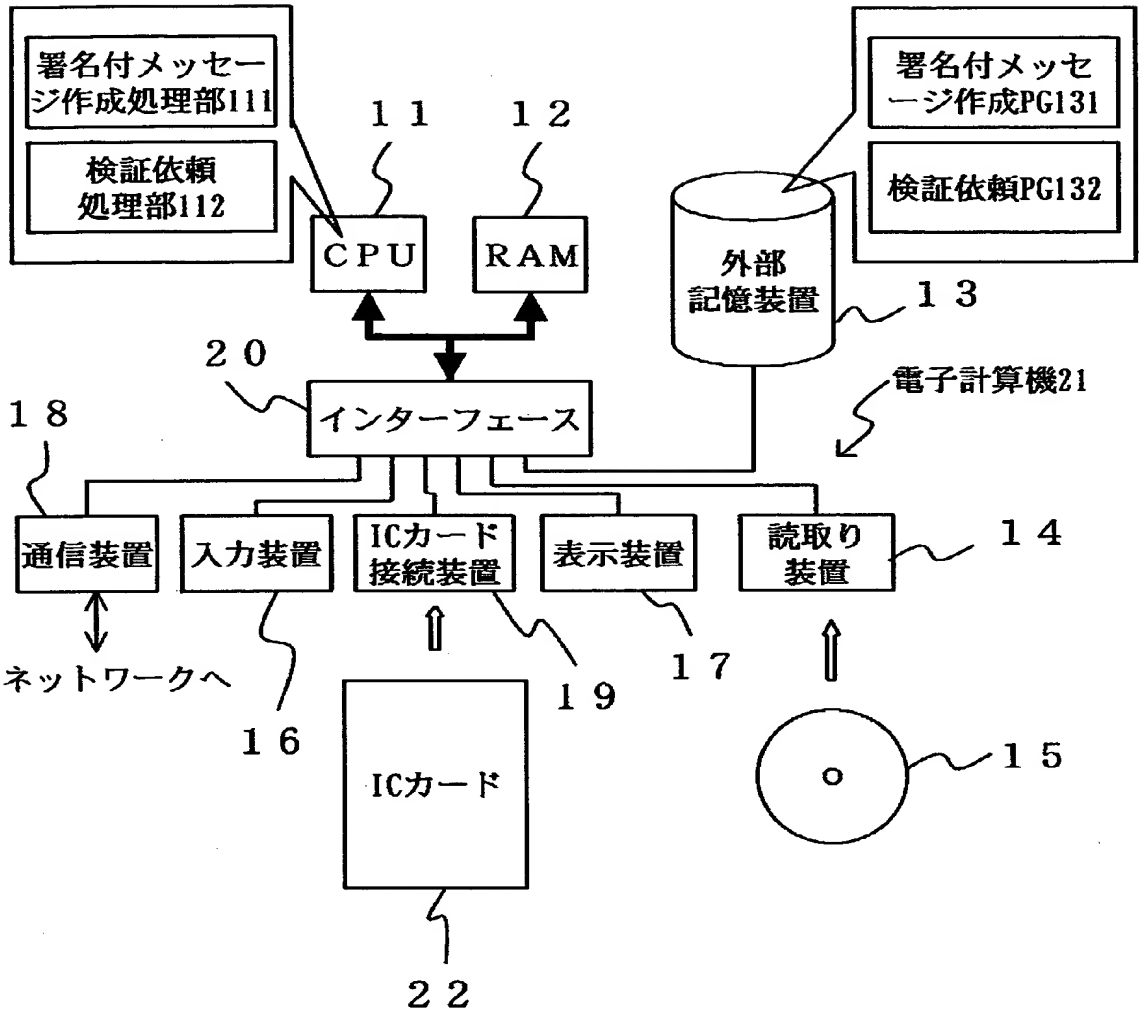
図１



出証特２０００－３０２６５２７

【図２】

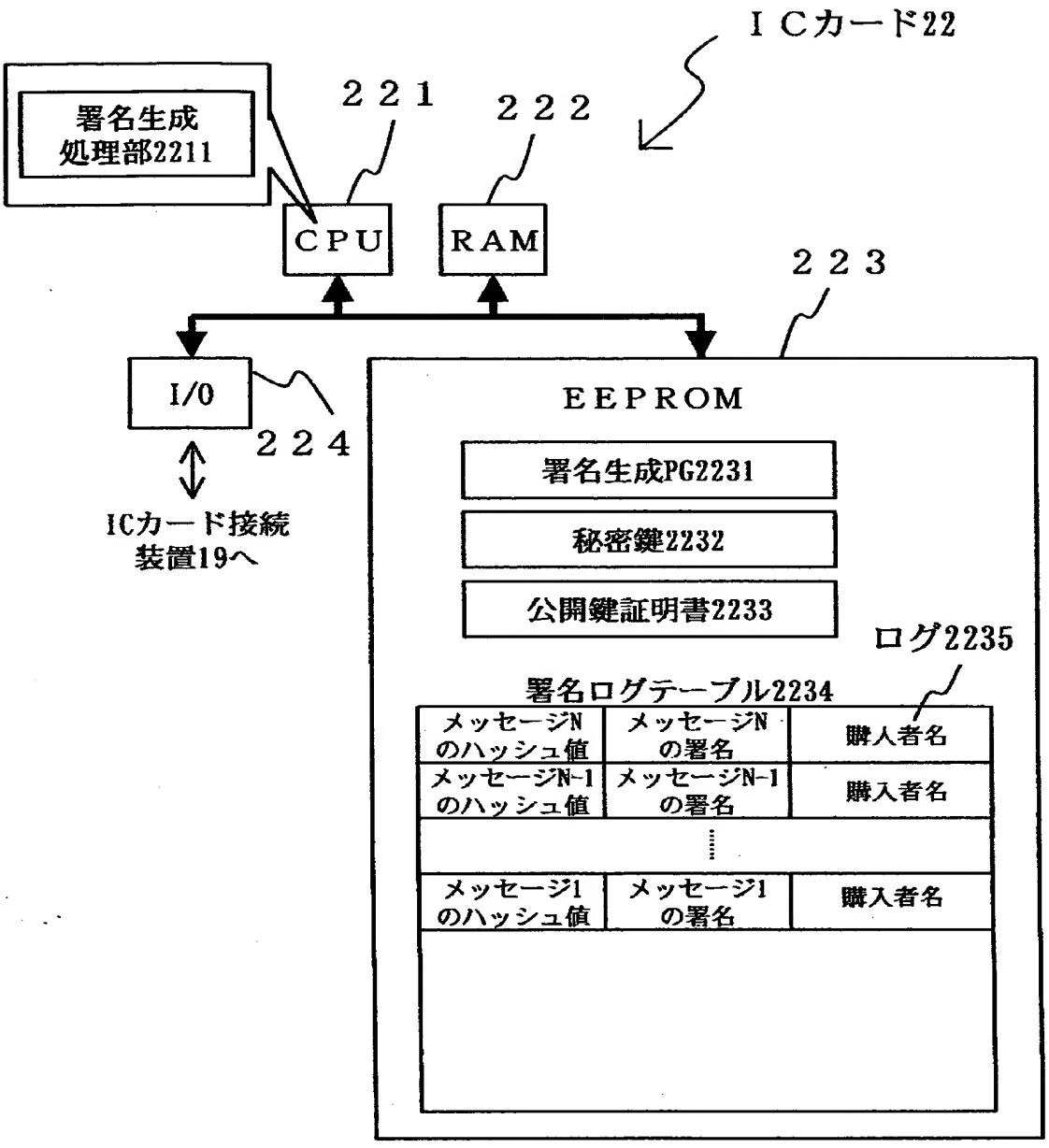
図２



デジタル署名者側装置１

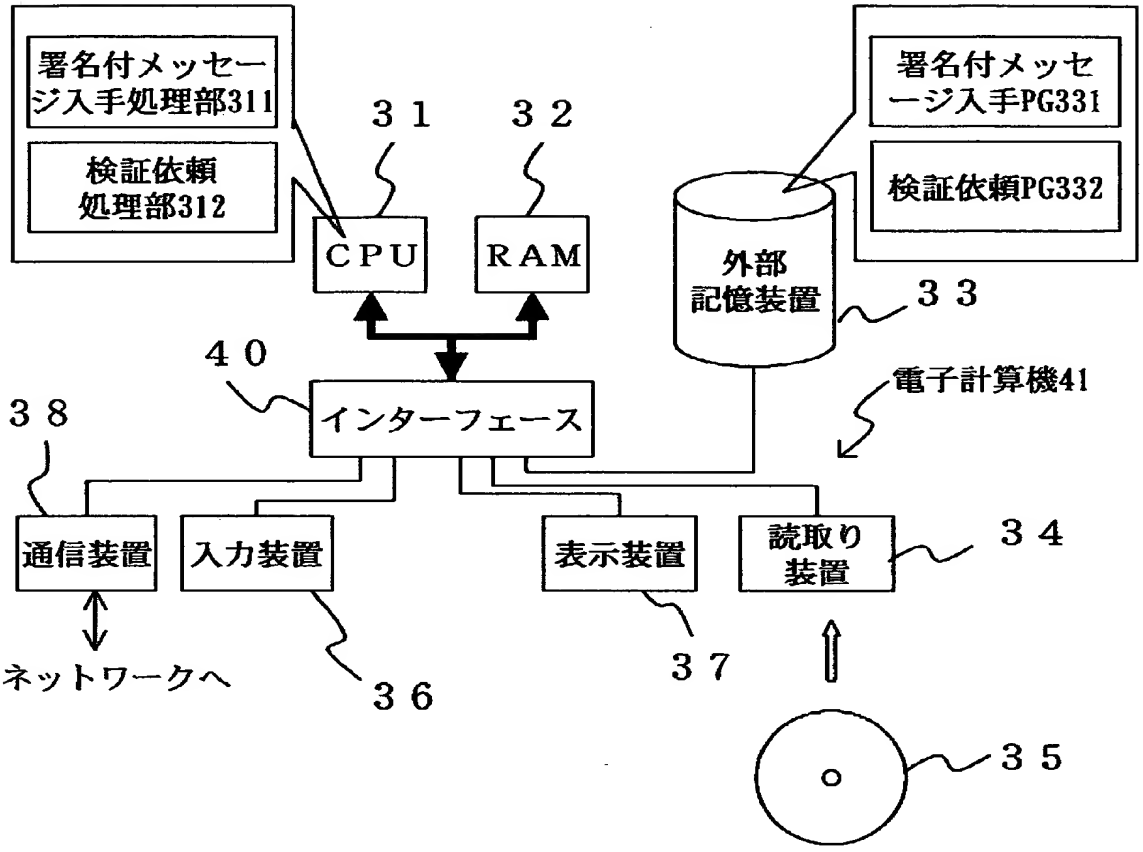
【図３】

図３


ＩＣカード22
２２１
２２２
２２３
署名生成
処理部2211
CPU
RAM
I/O
２２４
ICカード接続
装置19へ
EEPROM
署名生成PG2231
秘密鍵2232
公開鍵証明書2233
ログ2235
署名ログテーブル2234
メッセージN
のハッシュ値
メッセージN
の署名
購人者名
メッセージN-1
のハッシュ値
メッセージN-1
の署名
購入者名
メッセージ1
のハッシュ値
メッセージ1
の署名
購入者名

【図４】

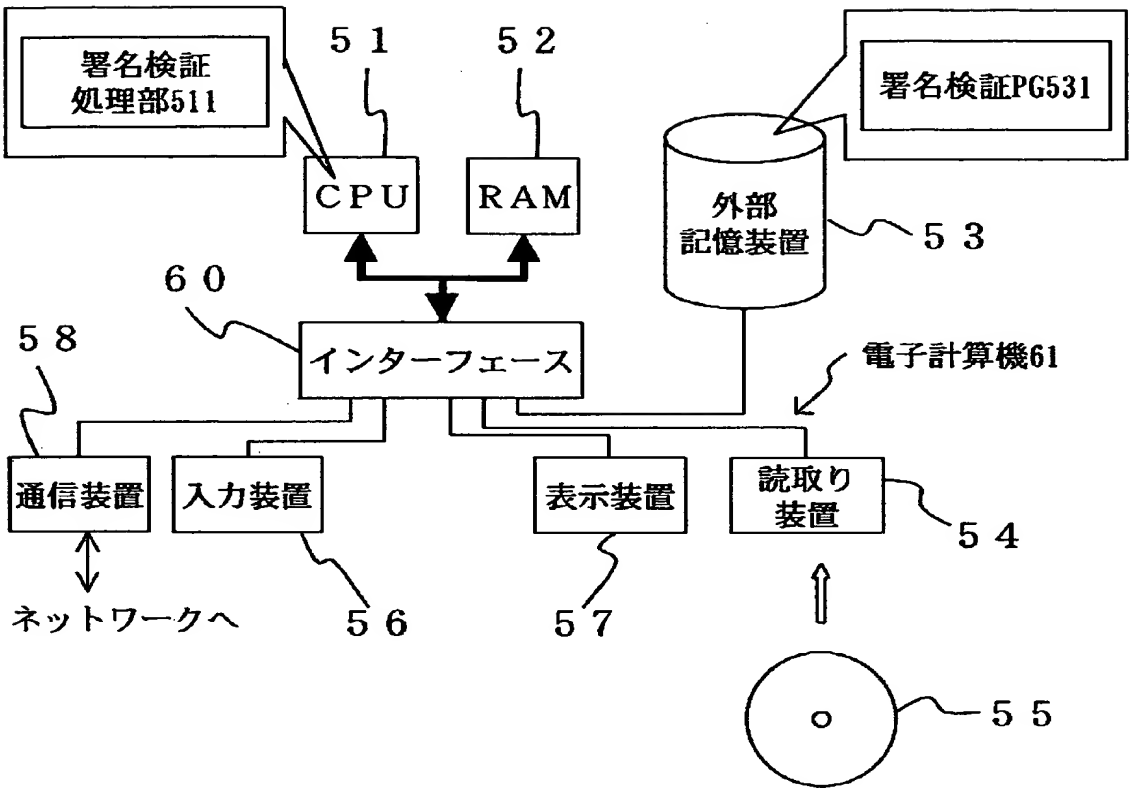
図４



購入者側装置３

【図５】

図５

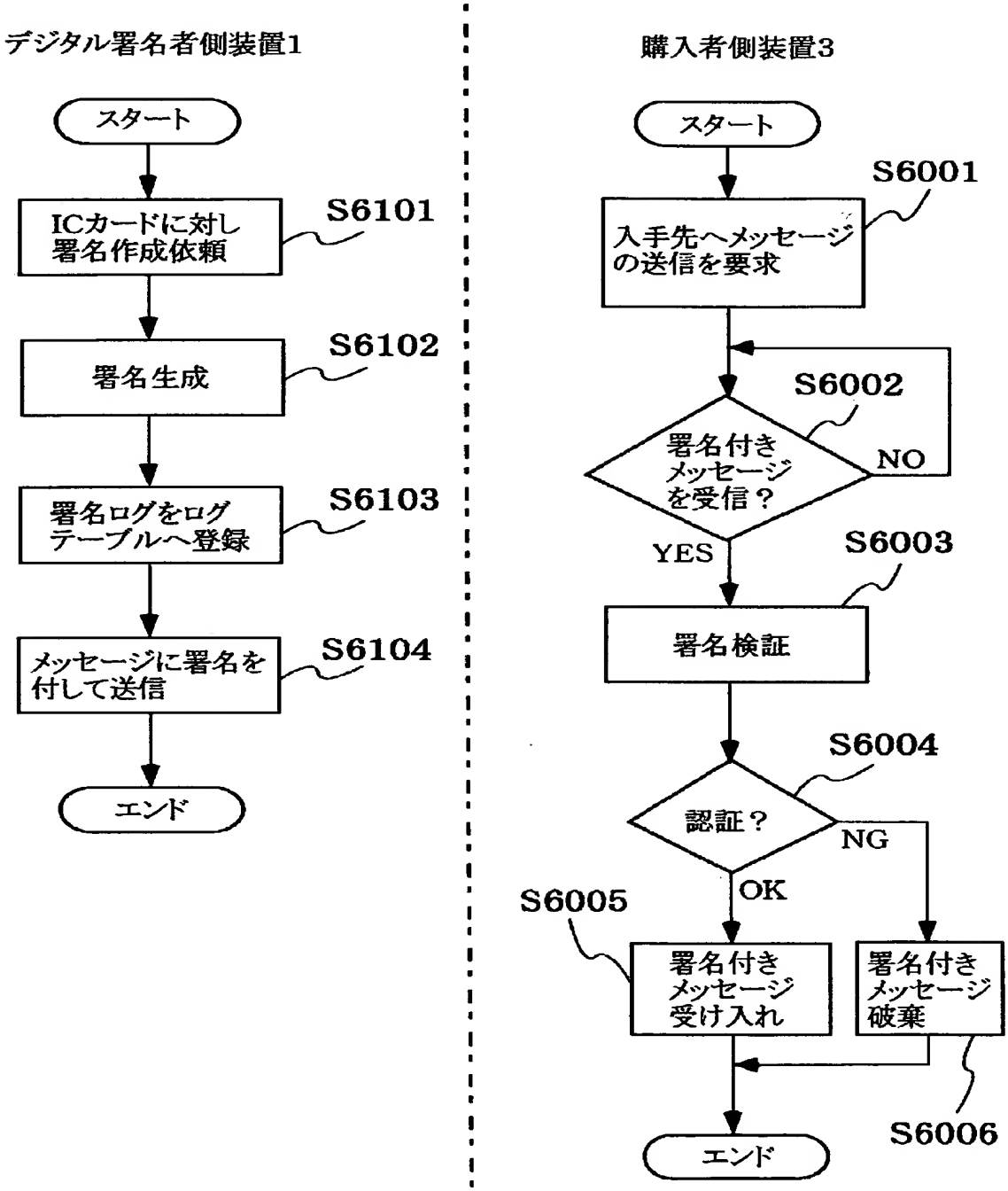


デジタル署名検証者側装置５

出証特２０００－３０２６５２７

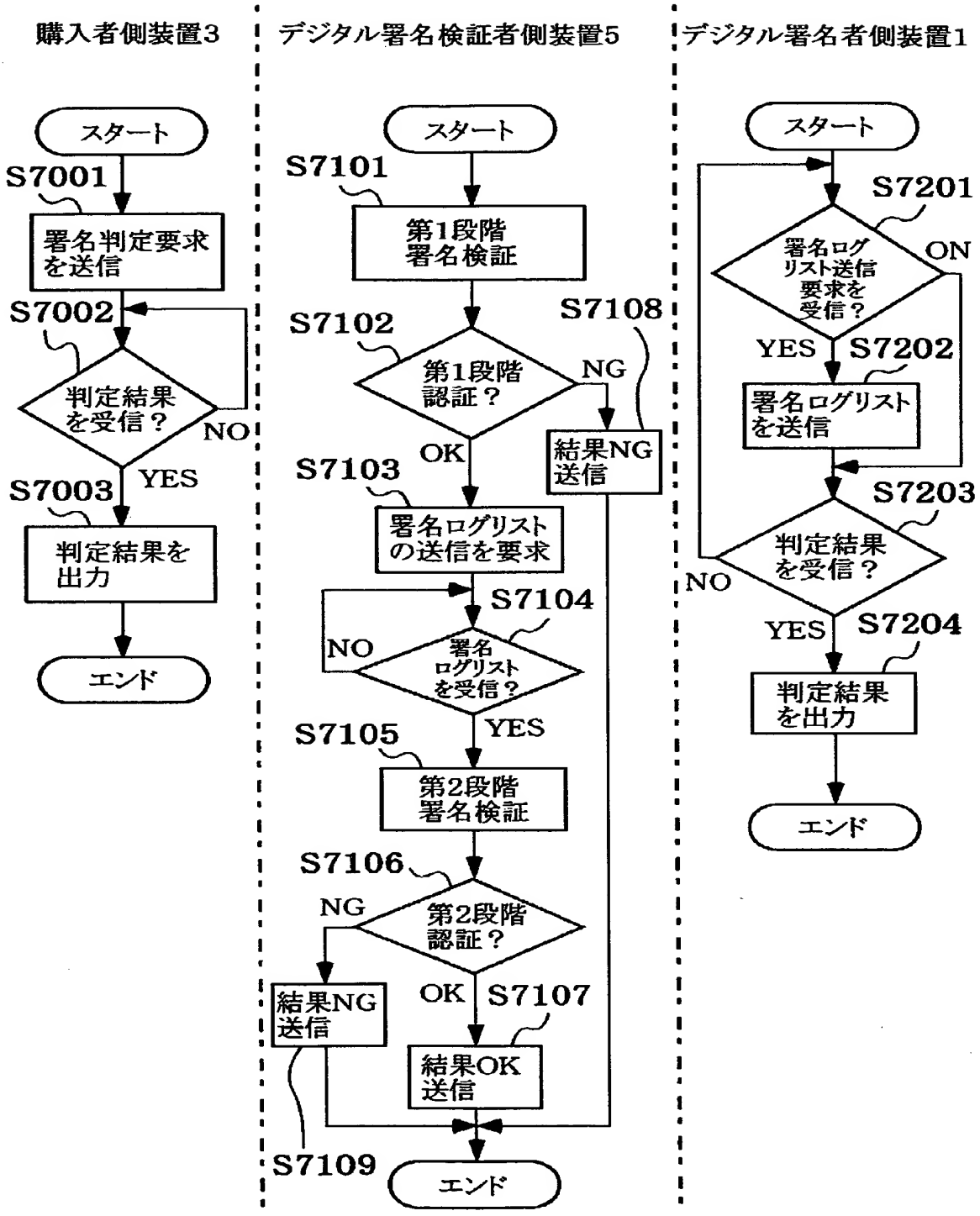
【図６】

図6


デジタル署名者側装置1
スタート
ICカードに対し署名作成依頼
S6101
署名生成
S6102
署名ログをログテーブルへ登録
S6103
メッセージに署名を付して送信
S6104
エンド
購入者側装置3
スタート
S6001
入手先へメッセージの送信を要求
S6002
署名付きメッセージを受信？
NO
YES
S6003
署名検証
S6004
認証？
NG
OK
S6005
署名付きメッセージ受け入れ
署名付きメッセージ破棄
S6006
エンド

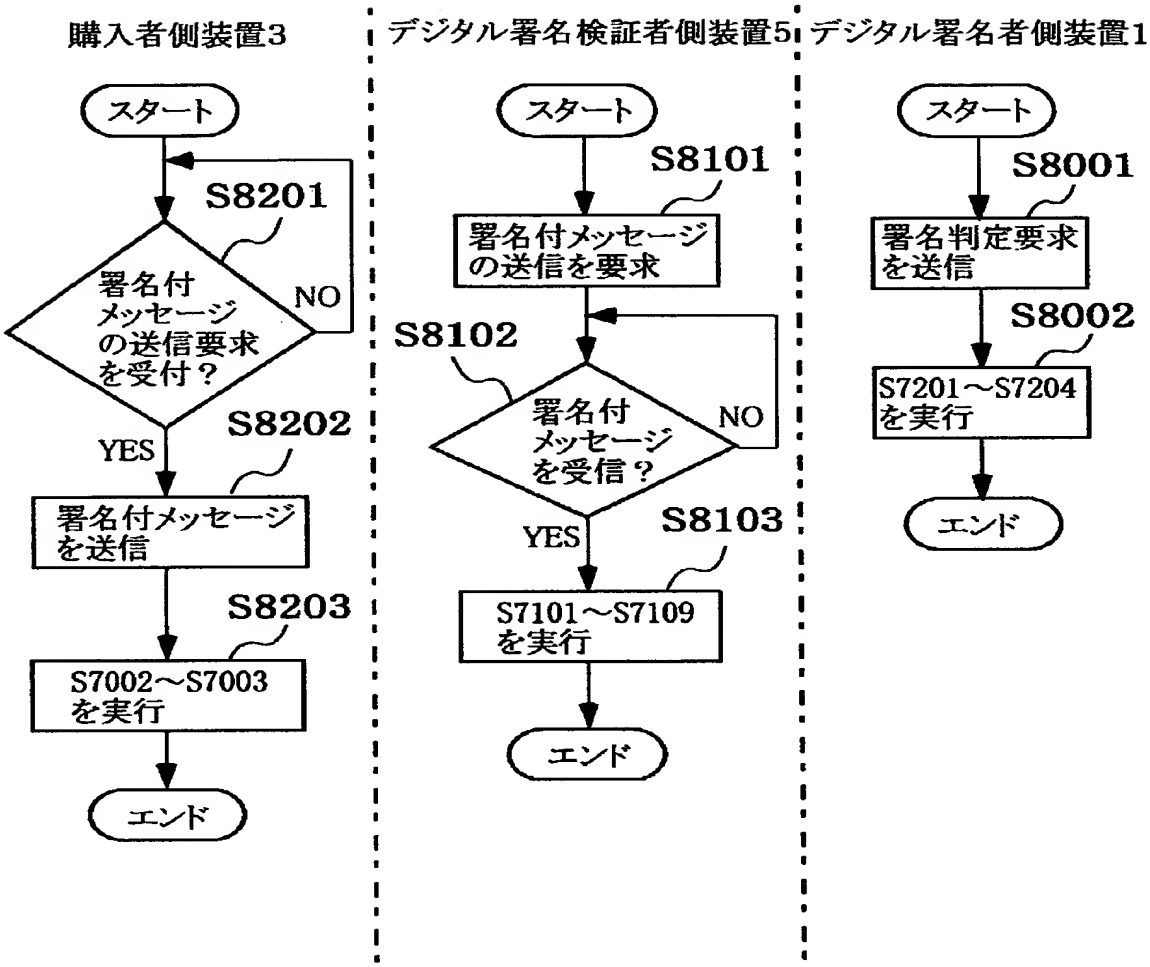
【図７】

図7


購入者側装置3
デジタル署名検証者側装置5
デジタル署名者側装置1
スタート
S7001
署名判定要求を送信
S7002
判定結果を受信？
NO
YES
S7003
判定結果を出力
エンド
スタート
S7101
第1段階署名検証
S7102
第1段階認証？
NG
S7108
結果NG送信
OK
S7103
署名ログリストの送信を要求
S7104
署名ログリストを受信？
NO
YES
S7105
第2段階署名検証
S7106
第2段階認証？
NG
結果NG送信
OK
S7107
結果OK送信
S7109
エンド
スタート
S7201
署名ログリスト送信要求を受信？
ON
YES
S7202
署名ログリストを送信
S7203
判定結果を受信？
NO
YES
S7204
判定結果を出力
エンド

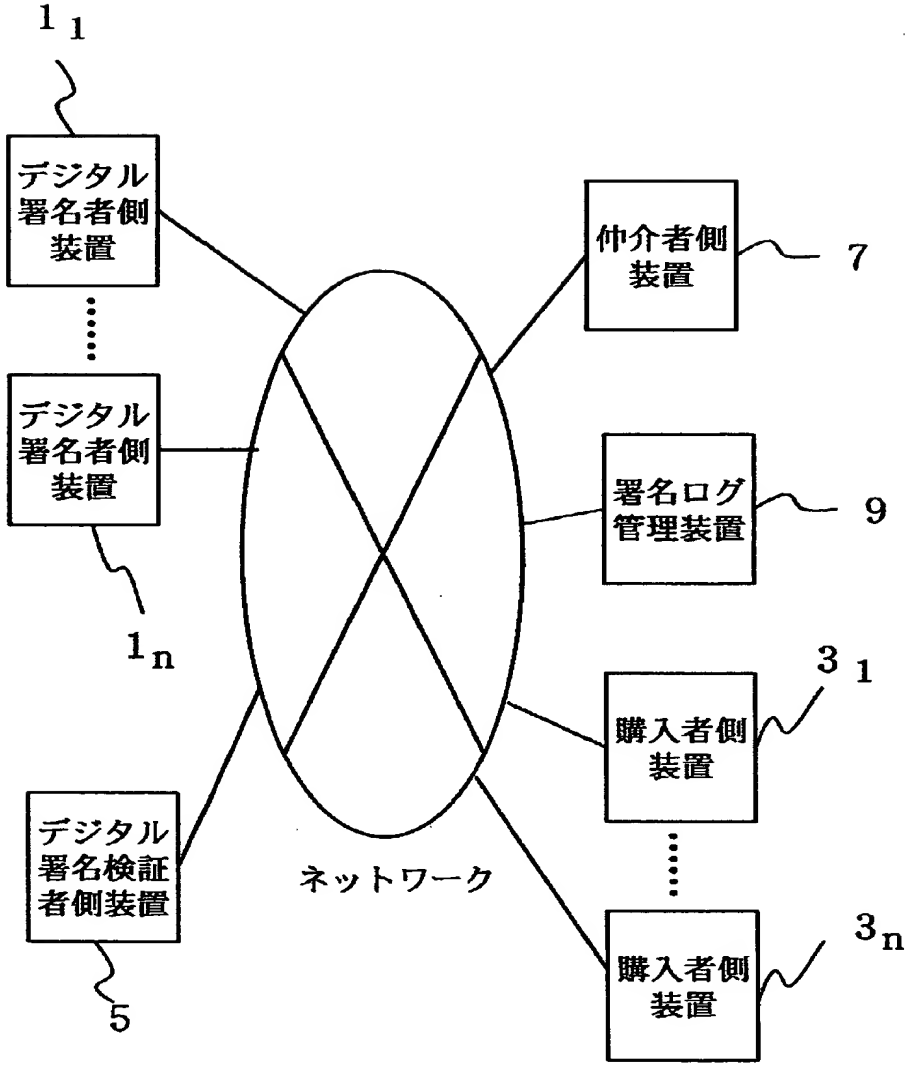
【図８】

図8


購入者側装置3
デジタル署名検証者側装置5
デジタル署名者側装置1
スタート
S8201
署名付メッセージの送信要求を受付？
NO
YES
S8202
署名付メッセージを送信
S8203
S7002～S7003を実行
エンド
スタート
S8101
署名付メッセージの送信を要求
S8102
署名付メッセージを受信？
NO
YES
S8103
S7101～S7109を実行
エンド
スタート
S8001
署名判定要求を送信
S8002
S7201～S7204を実行
エンド

【図９】

図９


1 1
デジタル署名者側装置
デジタル署名者側装置
1 n
デジタル署名検証者側装置
5
ネットワーク
仲介者側装置
7
署名ログ管理装置
9
3 1
購入者側装置
購入者側装置
3 n

【図１０】

図10

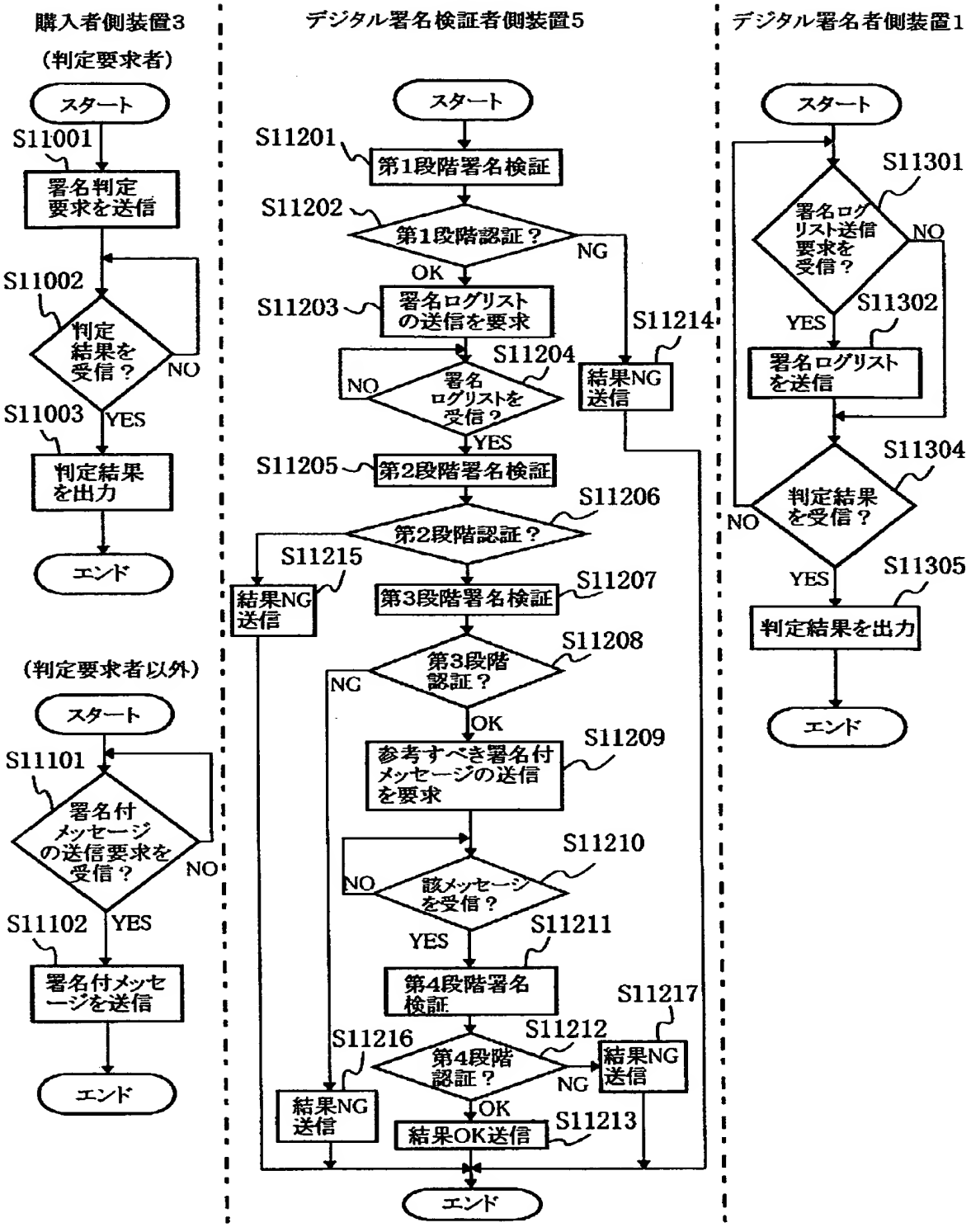
2235

署名ログテーブル2234

前データ (メッセージN-1)	メッセージN のハッシュ値	メッセージN の署名	購入者名
前データ (メッセージN-2)	メッセージN-1 のハッシュ値	メッセージN-1 の署名	購入者名
・ ・ ・ ・ ・			
前データ (メッセージ1)	メッセージ2 のハッシュ値	メッセージ2 の署名	購入者名
なし	メッセージ1 のハッシュ値	メッセージ1 の署名	購入者名

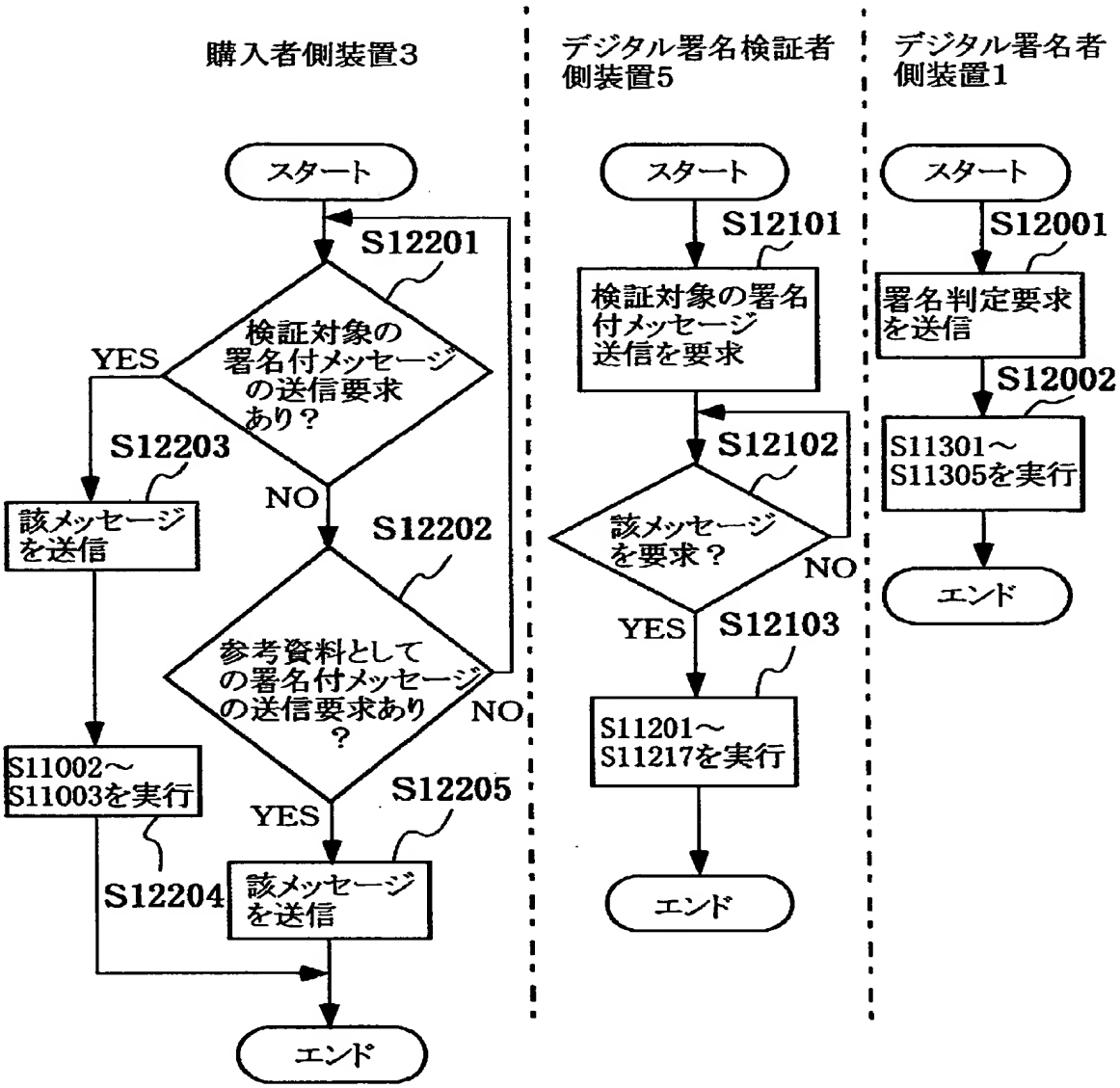
【図１１】

図11


購入者側装置3
（判定要求者）
スタート
S11001
署名判定要求を送信
S11002
判定結果を受信？
NO
YES
S11003
判定結果を出力
エンド
（判定要求者以外）
スタート
S11101
署名付メッセージの送信要求を受信？
NO
YES
S11102
署名付メッセージを送信
エンド
デジタル署名検証者側装置5
スタート
S11201
第1段階署名検証
S11202
第1段階認証？
NG
OK
S11203
署名ログリストの送信を要求
S11204
署名ログリストを受信？
NO
YES
S11205
第2段階署名検証
S11206
第2段階認証？
S11207
第3段階署名検証
S11208
第3段階認証？
NG
OK
S11209
参考すべき署名付メッセージの送信を要求
S11210
該メッセージを受信？
NO
YES
S11211
第4段階署名検証
S11212
第4段階認証？
NG
OK
S11213
結果OK送信
S11214
結果NG送信
S11215
結果NG送信
S11216
結果NG送信
S11217
結果NG送信
エンド
デジタル署名者側装置1
スタート
S11301
署名ログリスト送信要求を受信？
NO
YES
S11302
署名ログリストを送信
S11304
判定結果を受信？
NO
YES
S11305
判定結果を出力
エンド

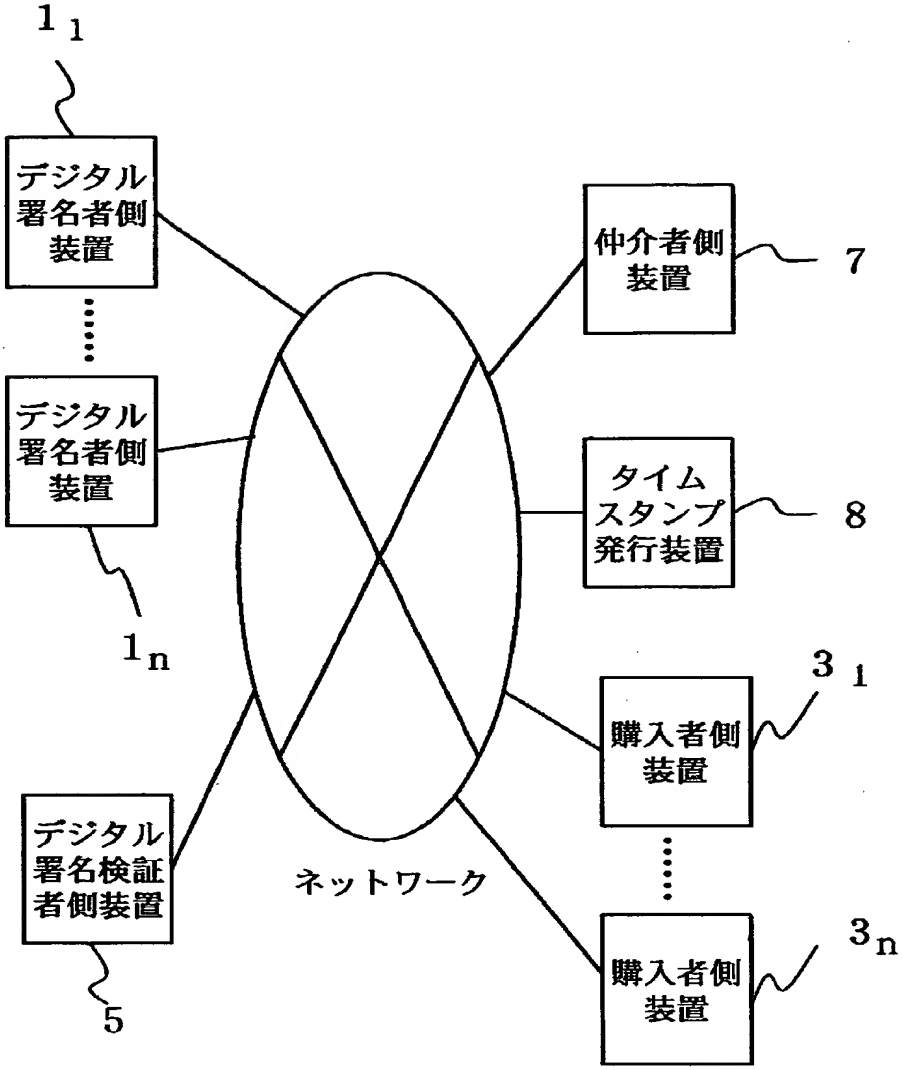
【図１２】

図12


購入者側装置3
デジタル署名検証者側装置5
デジタル署名者側装置1
スタート
S12201
検証対象の署名付メッセージの送信要求あり？
YES
NO
S12203
該メッセージを送信
S12202
参考資料としての署名付メッセージの送信要求あり？
NO
YES
S12205
該メッセージを送信
S11002～S11003を実行
S12204
エンド
スタート
S12101
検証対象の署名付メッセージ送信を要求
S12102
該メッセージを要求？
NO
YES
S12103
S11201～S11217を実行
エンド
スタート
S12001
署名判定要求を送信
S12002
S11301～S11305を実行
エンド

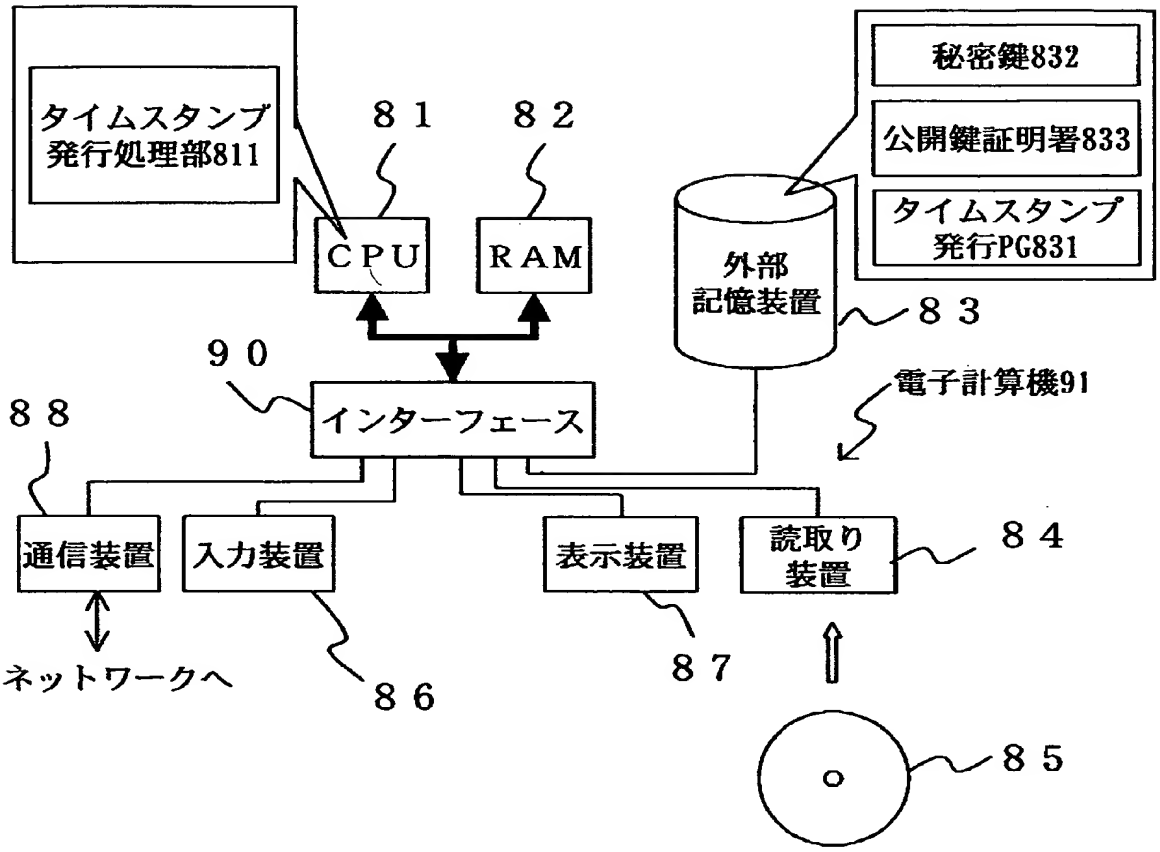
【図１３】

図１３


1 1
デジタル署名者側装置
デジタル署名者側装置
1 n
デジタル署名検証者側装置
5
ネットワーク
仲介者側装置
7
タイムスタンプ発行装置
8
購入者側装置
3 1
購入者側装置
3 n

【図１４】

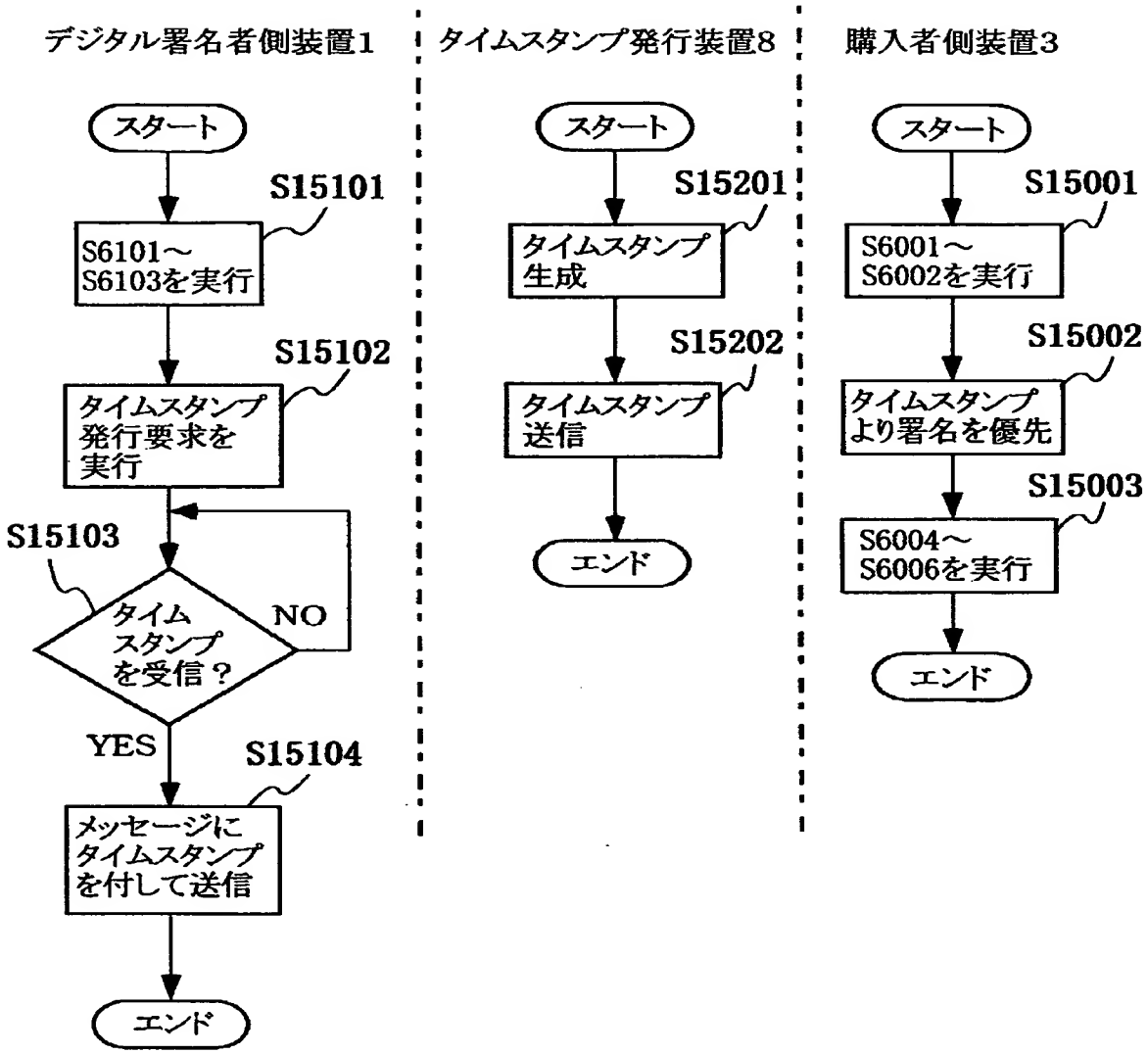
図１４



タイムスタンプ発行装置８

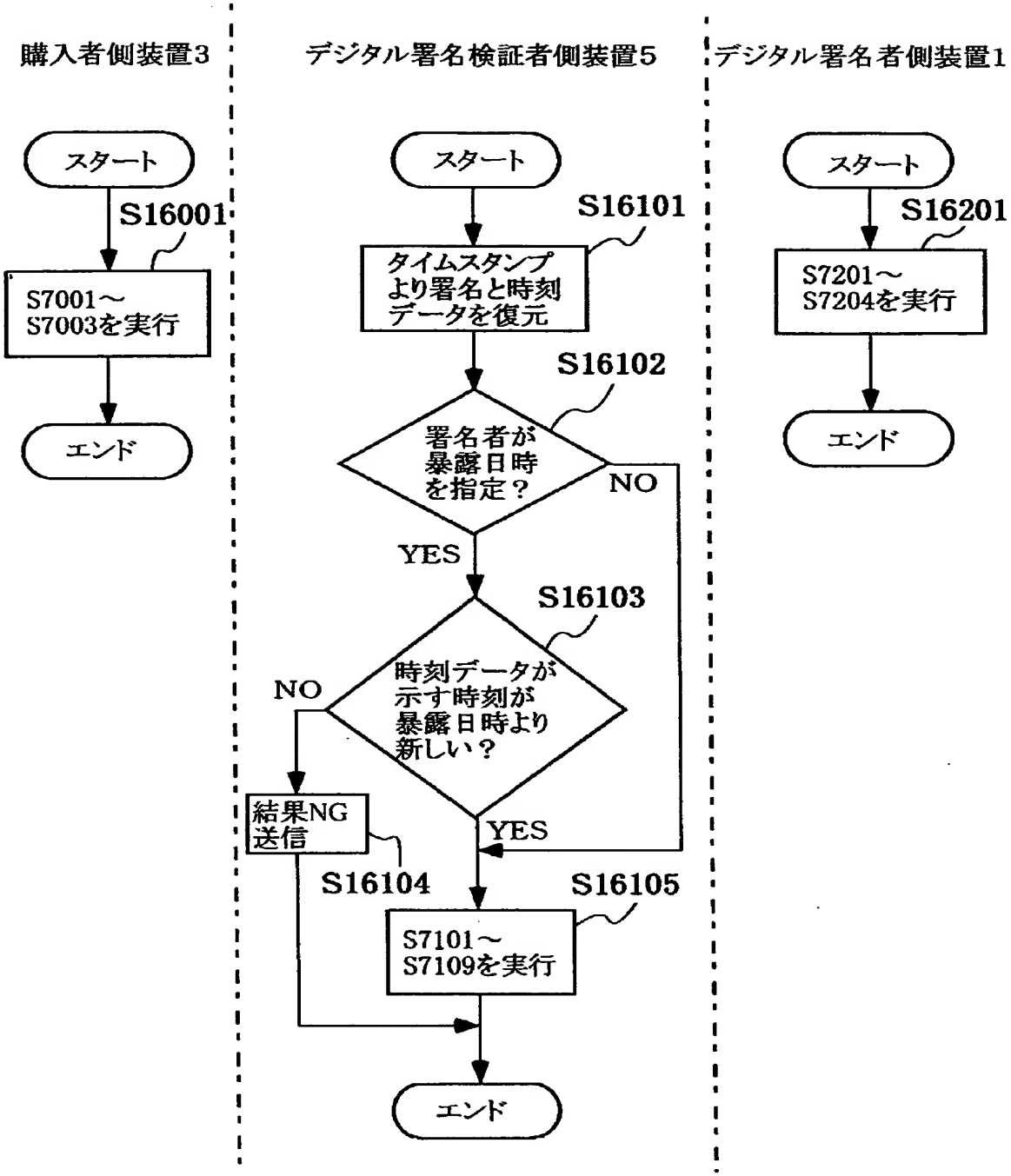
【図１５】

図15


デジタル署名者側装置1
タイムスタンプ発行装置8
購入者側装置3
スタート
S15101
S6101～
S6103を実行
S15102
タイムスタンプ
発行要求を
実行
S15103
タイム
スタンプ
を受信？
NO
YES
S15104
メッセージに
タイムスタンプ
を付して送信
エンド
スタート
S15201
タイムスタンプ
生成
S15202
タイムスタンプ
送信
エンド
スタート
S15001
S6001～
S6002を実行
S15002
タイムスタンプ
より署名を優先
S15003
S6004～
S6006を実行
エンド

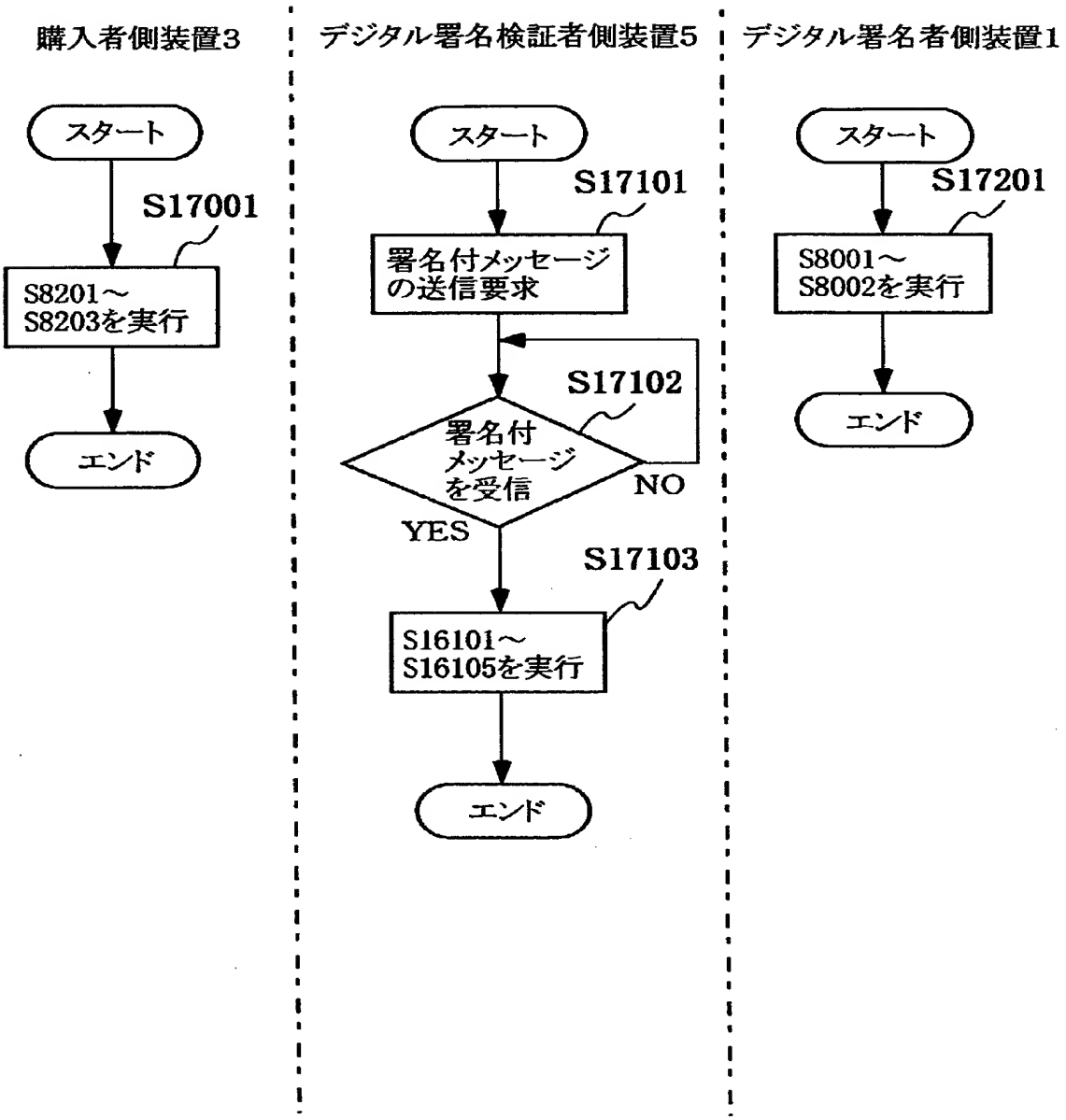
【図１６】

図16


購入者側装置3
デジタル署名検証者側装置5
デジタル署名者側装置1
スタート
S16001
S7001～
S7003を実行
エンド
スタート
S16101
タイムスタンプ
より署名と時刻
データを復元
S16102
署名者が
暴露日時
を指定？
NO
YES
S16103
時刻データが
示す時刻が
暴露日時より
新しい？
NO
YES
結果NG
送信
S16104
S16105
S7101～
S7109を実行
エンド
スタート
S16201
S7201～
S7204を実行
エンド

【図１７】

図17


購入者側装置3
デジタル署名検証者側装置5
デジタル署名者側装置1
スタート
S17001
S8201～
S8203を実行
エンド
スタート
S17101
署名付メッセージ
の送信要求
S17102
署名付
メッセージ
を受信
NO
YES
S17103
S16101～
S16105を実行
エンド
スタート
S17201
S8001～
S8002を実行
エンド

【図１８】

図18

署名ログテーブル2234　2235

メッセージN のハッシュ値	メッセージN の署名	購入者名	タイムスタンプ
メッセージN-1 のハッシュ値	メッセージN-1 の署名	購入者名	なし
・ ・ ・ ・ ・			
メッセージN-m のハッシュ値	メッセージN-m の署名	購入者名	タイムスタンプ
メッセージN-m-1 のハッシュ値	メッセージN-m-1 の署名	購入者名	なし
・ ・ ・ ・ ・			
メッセージ2 のハッシュ値	メッセージ2 の署名	購入者名	なし
メッセージ1 のハッシュ値	メッセージ1 の署名	購入者名	タイムスタンプ

【書類名】要約書

【要約】

【課題】デジタル署名生成者自身がしたデジタル署名と第３者がデジタル署名生成者になりすまして行ったデジタル署名とを識別可能とする。

【解決手段】デジタル署名者側装置1は、生成したデジタル署名とメッセージを含むデジタル署名付きメッセージの配布に先立ち、当該デジタル署名付きメッセージの署名ログ2235を署名ログテーブル2234に登録する。デジタル署名検証者側装置3は、デジタル署名者側装置1から署名ログリストを入手し、検証対象のデジタル署名付きメッセージが取得した署名ログリストに登録されているか否かを調べることで、当該デジタル署名付きメッセージがデジタル署名者側装置１で生成されたものであるか否かを検証する。

【選択図】図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所